

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004年7月29日 (29.07.2004)

PCT

(10) 国際公開番号
WO 2004/064317 A1

- (51) 国際特許分類⁷: H04L 9/32, G11B 20/10, G06F 12/14
- (21) 国際出願番号: PCT/JP2003/016226
- (22) 国際出願日: 2003年12月18日 (18.12.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2003-6915 2003年1月15日 (15.01.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 村松 克美 (MURAMATSU, Katsumi) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 杉浦 正知, 外 (SUGIURA, Masatomo et al.); 〒171-0022 東京都豊島区南池袋2丁目49番7号 池袋パークビル7階 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

添付公開書類:

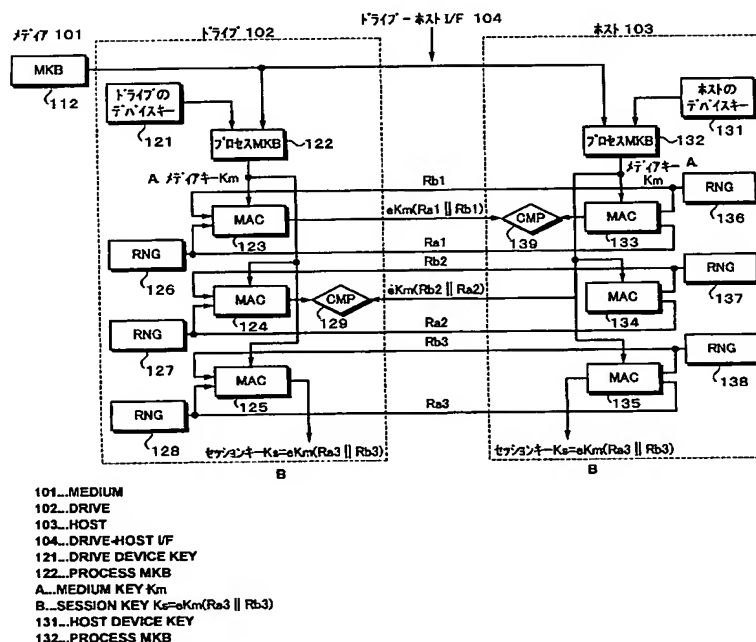
— 国際調査報告書

— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

[続葉有]

(54) Title: MUTUAL AUTHENTICATION METHOD, PROGRAM, RECORDING MEDIUM, SIGNAL PROCESSING SYSTEM, REPRODUCTION DEVICE, AND INFORMATION PROCESSING DEVICE

(54) 発明の名称: 相互認証方法、再生装置及び情報処理装置



(57) Abstract: An MKB and a device key (121) of a drive are input to a process MKB. The drive is subjected to revoke processing and a host (103) is revoked by a process MKB (132). MAC values calculated by MAC calculation blocks (123, 133) are compared in the host (103). If the two values are judged to be identical, the authentication of the drive (102) by the host (103) is successful. MAC values calculated

[続葉有]



2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

by MAC calculation blocks (134, 124) of the host (103) are compared in the drive (102). If the two values are judged to be identical, authentication of the host (103) by the drive (102) is successful. When the mutual authentication is successful, a common session key is generated by MAC calculation blocks (125, 135).

(57) 要約: プロセスMKB 1 2 2にMKBとドライブの持つデバイスキー 1 2 1とが入力され、ドライブがリボーク処理され、プロセスMKB 1 3 2によってホスト 1 0 3がリボーク処理される。MAC演算ブロック 1 2 3および 1 3 3が演算したMAC値がホスト 1 0 3内において比較され、二つの値が同一と判定されると、ホスト 1 0 3によるドライブ 1 0 2の認証が成功したことになる。ホスト 1 0 3のMAC演算ブロック 1 3 4および 1 2 4が演算したMAC値がドライブ 1 0 2内において比較され、二つの値が同一と判定されると、ドライブ 1 0 2によるホスト 1 0 3の認証が成功したことになる。相互認証が成功すると、MAC演算ブロック 1 2 5および 1 3 5によって、共通のセッションキーが生成される。

相互認証方法、再生装置及び情報処理装置

相互認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置

5

技術分野

この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディアに暗号化コンテンツを記録し、また、ディスクメディアから暗号化コンテンツを再生する場合に適用される相互

10 認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置に関する。

背景技術

近年開発されたDVD (Digital Versatile Disc)等の記録媒体では
15 、1枚の媒体に例えば映画1本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となると不正コピーを防止して著作権の保護を図ることがますます重要となっている。

DVD-Videoでは、コピープロテクション技術としてCSS (Content Scrambling System) が採用されている。CSSは、DVD-ROMメディアに対する適用のみが認可されており、DVD-R、DVD-RW、DVD+R、DVD+RW等の記録型DVDでのCSSの利用がCSS契約によって禁止されている。したがって、CSS方式で著作権保護されたDVD-Videoの内容を記録型DVDへのま
20 るごとコピー（ビットバイビットコピー）することは、CSS契約上では
25 、認められた行為ではない。

しかしながら、C S S の暗号方式が破られる事態が発生した。C S S の暗号化を解除してD V D -Video の内容を簡単にハードディスクにコピーすることを可能とする「D e C S S」と呼ばれるソフトウェアがインターネット上で配布された。「D e C S S」が出現した背景
5 には、本来耐タンパー化が義務付けられているはずのC S S 復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的にC S S アルゴリズム全体が解読された経緯がある。

C S S の後に、D V D -Audio 等のD V D -R O M の著作権保護技術であるC P P M (Content Protection for Pre-Recorded Media) 、
10 並びに記録型D V D 、メモ리카ードに関する著作権保護技術C P R M (Content Protection for Recordable Media) が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、システムを更新でき、データをまるごとコピーしても再生
15 を制限できる特徴を有している。D V D に関する著作権保護の方法に関しては、下記の非特許文献1に説明され、C P R M は、ライセンス管理者である米4C Entity, LLC が配布する下記の資料に説明されている。

山田, 「D V D を起点に著作権保護空間を広げる」, 日経エレクトロ
20 ニクス 2001. 8. 13, p. 143-153

"Content Protection for Recordable Media Specification DVD Book", インターネット<URL : <http://www.4Centity.com/>>

パーソナルコンピュータ(以下、適宜P C と略す)環境下では、P C とドライブとが標準的インターフェースで接続されるために、標準
25 的インターフェースの部分で秘密保持が必要なデータが知られたり、データが改ざんされるおそれがある。アプリケーションソフトウェア

がリバースエンジニアリングされ、秘密情報が盗まれたり、改ざんされる危険がある。このような危険性は、記録再生装置が一体に構成された電子機器の場合では、生じることが少ない。

著作権保護技術をP C上で実行されるアプリケーションプログラム
5 へ実装する際には、その著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的である。しかしながら、耐タンパー性の強度を示す指標がない。その結果、どの程度のリバースエンジニアリングへの対応を行うかは、インプレメンターの個々の判断や能力に委ねられているのが現状である。C S Sの場合は、結果としてその著作権保
10 護技術が破られてしまった。C S Sの後に提案されたC P P Mおよび記録型D V Dに関する著作権保護技術C P R Mにおいても、既に破られているC S Sに新たな機能を加えたものであり、また、著作権保護技術に関わるアルゴリズムは、大部分がP Cでの実装に依存するものであり、コンテンツプロテクションの機能が十分に強いものと言えない
15 い問題があった。すなわち、アプリケーションソフトウェアなどのリバースエンジニアリングによって、著作権保護技術に関わる秘密情報の解析により暗号方式が破られ、ディスクからのデータとしてP Cがそのまま読み出した暗号化コンテンツが「D e C S S」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとして
20 てコピー制限の働かない状態で複製が繰り返されるような事態を招くことで、著作権保護が機能しなくなるという危険性があった。

この発明の目的は、P C環境下でも著作権保護技術の安全性を確保することができる相互認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置を提供することにある。

25

発明の開示

上述した課題を解決するために、この発明の第 1 の態様は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法において、

- 再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第 1 の判定ステップを有し、
- 10 情報処理装置は、当該情報処理装置を表す情報とリボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第 2 の判定ステップを有し、

第 1 の判定ステップによって無効化すべきという判定をされなかった場合に生成される第 1 の鍵情報と、第 2 の判定ステップによって無効化すべきという判定をされなかった場合に生成される第 2 の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法である。

15

この発明の第 2 の態様は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムであって、

20

- 再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第 1 の判定ステップを有し、
- 25

情報処理装置は、当該情報処理装置を表す情報とリボケーション情

報を用いて当該情報処理装置を無効化すべきか否かを判定する第 2 の判定ステップを有し、

第 1 の判定ステップによって無効化すべきという判定をされなかった場合に生成される第 1 の鍵情報と、第 2 の判定ステップによって無効化すべきという判定をされなかった場合に生成される第 2 の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプログラムである。

この発明の第 3 の態様は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムを格納した記録媒体であって、

15 再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第 1 の判定ステップを有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第 2 の判定ステップを有し、

第 1 の判定ステップによって無効化すべきという判定をされなかった場合に生成される第 1 の鍵情報と、第 2 の判定ステップによって無効化すべきという判定をされなかった場合に生成される第 2 の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプログラムを格納した記録媒体である。

この発明の第 4 の態様は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置とを
5 備える信号処理システムであって、

再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第 1 の判定手段を有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第 2
10 の判定手段を有し、

第 1 の判定手段によって無効化すべきという判定をされなかった場合に生成される第 1 の鍵情報と、第 2 の判定手段によって無効化すべきという判定をされなかった場合に生成される第 2 の鍵情報とを用い
15 て、再生装置と情報処理装置とが相互に認証する相互認証手段と、

相互認証手段による相互認証後に、再生装置および情報処理装置に共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする信号処理システムである。

この発明の第 5 の態様は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有し、コンテンツ情報が伝達手段を介して情報処理装置に送信され、処理される信号処理システムにおける再生装置であって、
20

当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第 1 の判定手段を有し、
25

第 1 の判定手段によって無効化すべきという判定をされなかった場

合に生成される第 1 の鍵情報と、

情報処理装置に設けられている当該情報処理装置を表す情報とリボ
ケーション情報とを用いて当該情報処理装置を無効化すべきか否かを
判定する第 2 の判定手段によって無効化すべきという判定をされなか
5 った場合に生成される第 2 の鍵情報とを用いて、情報処理装置と相互
に認証する相互認証手段と、

相互認証手段による相互認証後に、情報処理装置と共通の共通鍵を
生成する共通鍵生成手段とを備えることを特徴とする再生装置である
。

10 この発明の第 6 の態様は、不正な電子機器を判別するためのリボケ
ーション情報と記録媒体固有の情報とを予め備えた記録媒体から、再
生装置がコンテンツ情報を読み出し、コンテンツ情報が伝達手段を介
して受信され、処理される情報処理装置であって、

再生装置に設けられている第 1 の判定手段によって、当該再生装置
15 を表す情報とリボケーション情報とを用いて当該再生装置を無効化す
べきか否かを判定し、第 1 の判定手段によって無効化すべきという判
定をされなかった場合に生成される第 1 の鍵情報と、

当該情報処理装置を表す情報とリボケーション情報とを用いて当該
情報処理装置を無効化すべきか否かを判定する第 2 の判定手段を有し
20 、

第 1 の鍵情報と、第 2 の判定手段によって無効化すべきという判定
をされなかった場合に生成される第 2 の鍵情報とを用いて、再生装置
と相互に認証する相互認証手段と、

相互認証手段による相互認証後に、再生装置と共通の共通鍵を生成
25 する共通鍵生成手段とを備えることを特徴とする情報処理装置である
。

この発明では、メディア上に記録された鍵情報（M K B）と各デバイスまたは各アプリケーションに記憶されている鍵情報（デバイスキー）から同一の値として導かれる鍵情報（メディアキー）を利用して相互認証がなされる。したがって、この発明においては、認証のため
5 だけに用意される特定の認証鍵を必要とせず、秘密情報を少なくでき、また、デバイスまたはアプリケーションによってデバイスキーを異ならせることが可能であるので、秘密情報が不正に読み取られる危険性を少なくできる。

この発明では、著作権保護技術に関する秘密情報である電子機器またはアプリケーションソフトウェア固有の情報例えばデバイスキーが
10 ドライブ内に実装されているので、情報処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著
15 作権保護技術の安全性を確保することができる。

電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリポークすることが可能となる。さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばL S Iによっ
20 て生成できるので、P C内でソフトウェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少なくできる。

25 図面の簡単な説明

第1図は、先に提案されているレコーダ、プレーヤおよびD V Dメ

ディアからなるシステムを説明するためのブロック図である。

第 2 図は、P C ベースの D V D メディア記録再生システムを説明するためのブロック図である。

第 3 図は、第 2 図のシステムにおける D V D ドライブ 4 およびホス
5 ト 5 の処理の手順を説明するための略線図である。

第 4 図は、第 2 図のシステムにおける認証動作を説明するためのフ
ローチャートである。

第 5 図は、この発明の一実施形態による相互認証のための構成を示
すブロック図である。

10 第 6 図は、この発明の一実施形態におけるドライブの認証動作の処
理の手順を説明するためのフローチャートである。

第 7 図は、この発明の一実施形態におけるホストの認証動作の処理
の手順を説明するためのフローチャートである。

第 8 図は、この発明の一実施形態によるドライブとホストを組み合
15 わせたレコーダの構成の一例をブロック図である。

第 9 図は、レコーダの一例の通信の手順を説明するための略線図で
ある。

第 1 0 図は、この発明の一実施形態によるドライブとホストを組み
合わせたプレーヤの構成の一例をブロック図である。

20 第 1 1 図は、プレーヤの一例の通信の手順を説明するための略線図
である。

第 1 2 図は、この発明の一実施形態によるドライブとホストを組み
合わせたレコーダの構成の他の例をブロック図である。

第 1 3 図は、レコーダの他の例の通信の手順を説明するための略線
25 図である。

発明を実施するための最良の形態

この発明の一実施形態の説明に先立って、本明細書の特許請求の範囲において使用される用語と実施の形態中で使用される用語との対応関係について以下に説明する。

- 5 記録媒体：メディア例えばディスク、再生装置：ドライブ、情報処理装置：ホスト、伝達手段：ドライバ－ホストインターフェース、信号処理システム：メディアを再生するドライブとホストとがドライバ－ホストインターフェースを介して接続されるシステムである。第1の送信手段：ドライブ側からセッションキーを共通鍵とした共通鍵暗号方式で情報をホスト側に送る手段、第2の送信手段：逆にホスト側からセッションキーを共通鍵として情報をドライブ側に送る手段のことである。

- コンテンツ情報：メディアに記録されている情報または記録すべき情報をコンテンツ情報としている。リボケーション情報：メディアに
15 予め記録されているメディアキーブロックMKB(Media Key Blocks)、記録媒体固有の情報：メディアID、デバイスキー：再生装置または情報処理装置を表す情報、装置を無効化すべきか否かを判定する判定手段：プロセスMKBである。プロセスMKBでは、ドライブ側の第1の判定手段によりドライブが無効化されなければ、ドライブ側の
20 メディアキーとして第1の鍵情報が生成され、ホスト側の第2の判定手段によりホストが無効化されなければ、ホスト側のメディアキーとして第2の鍵情報が生成される。ドライブとホストは、独立して無効化が可能であり、無効化された場合は、期待されるメディアキーを得ることができないので「第1の」、「第2の」と分けている。
- 25 相互認証手段：AKE(Authentication and Key Exchange)（プロセスMKB以降の乱数交換、MAC計算、比較からなるドライブ側の

第1の確認手段とホスト側の第2の確認手段により相互に相手の動作を確認することである。ドライブ側とホスト側の何れが先に確認するかの順番は、任意であるので、用語の統一を図るために、ドライブ側の確認手段を「第1の」としている。）

- 5 共通鍵：セッションキー（確実に暗号化・復号に使われるセッションキーとコンテンツキーとは、「鍵」でそれ以外は「鍵情報」として
いる。認証完了後なので共通鍵として同じ暗号化鍵が生成されるが、
生成している装置と、基にしている鍵情報の呼び方を変えていること
から、ドライブ側の生成手段を第1の共通鍵生成手段、ホスト側の生
10 成手段を第2の共通鍵生成手段としている。）

- 乱数を生成する乱数生成手段：乱数発生器（RNG：Random Number Generator）（ドライブ側の乱数生成手段を第1の乱数生成手段、ホ
スト側の乱数生成手段を第2の乱数生成手段とし、特許請求の範囲に
おいては、生成される乱数に対して請求の範囲に出てくる順番で番号
15 をつけている。）

所定の計算を行う計算手段：MAC (Message Authentication Code)
演算ブロック（乱数交換手段により交換された乱数を用いて、ドラ
イブ側で計算する手段を第1の計算手段、ホスト側の計算手段を第2
の計算手段としている。）

- 20 比較手段：比較（ドライブ側の比較を第1の比較手段、ホスト側の
比較を第2の比較手段としている。）

- 記録媒体固有の鍵情報：メディアユニークキー（本実施形態におい
ては、メディアユニークキーの生成は耐タンパー性を持たせるために
全てドライブ側で行われているので、記録媒体固有の鍵情報（メ
25 ディアユニークキー）を生成する中間鍵生成手段は、ドライブ側のみとし
ている。）

コンテンツ情報暗号化鍵またはコンテンツ情報復号鍵の基になる鍵情報：（記録時に使われるタイトルキーを第3の鍵情報、再生時に使われるタイトルキーを第4の鍵情報としている。メディアユニークキーによってタイトルキーを暗号化する手段を鍵情報暗号化手段、復号する手段を鍵情報復号手段としている。メディアユニークキーによって暗号化されたタイトルキーを記録媒体に記録する手段を暗号化鍵情報記録手段としている。）

コンテンツ情報を暗号化または復号するための鍵：コンテンツキー（記録時に使われるコンテンツキーをコンテンツ情報暗号化鍵とし、再生時に使われるコンテンツキーをコンテンツ情報復号鍵としている。コンテンツ情報暗号化鍵を生成する手段を最終暗号化鍵生成手段、コンテンツ情報復号鍵を生成する手段を最終復号鍵生成手段としている。暗号化されたコンテンツ情報を記録媒体に記録する手段をコンテンツ情報記録手段とし、暗号化されたコンテンツ情報を復号する手段をコンテンツ情報復号手段としている。）

次に、この発明の理解の容易のために、最初に第1図を参照して著作権保護技術例えばDVD用CPRMのアーキテクチャについて説明する。第1図において、参照符号1が例えばCPRM規格に準拠したDVD-R/RW、DVD-RAM等の記録型DVDメディアを示す。参照符号2が例えばCPRM規格に準拠したレコーダを示す。参照符号3が例えばCPRM規格に準拠したプレーヤを示す。レコーダ2およびプレーヤ3は、機器またはアプリケーションソフトウェアである。

未記録ディスクの状態において、DVDメディア1の最内周側のリードインエリアのBCA (Burst Cutting Area) またはNBCA (Narrow Burst Cutting Area) と称されるエリアには、メディアID11が

記録されている。リードインエリアのエンボスまたはプリ記録データゾーンには、メディアキーブロック（以下、MKBと適宜略す）12が予め記録されている。メディアID11は、個々のメディア単位例えばディスク1枚毎に異なる番号であり、メディアの製造者コードと
5 シリアル番号から構成される。メディアID11は、メディアキーを個々のメディアで異なるメディアユニークキーへ変換する際に必要となる。メディアキーブロックMKBは、メディアキーの導出、並びに機器のリボケーション（無効化）を実現するための鍵束である。これらのメディアIDおよびメディアキーブロックは、記録媒体固有の第
10 1の情報である。

ディスク1の書き換えまたは追記可能なデータ領域には、コンテンツキーで暗号化された暗号化コンテンツ13が記録される。暗号化方式としては、C2 (Cryptomeria Cipherng) が使用される。

DVDメディア1には、暗号化タイトルキー14およびCCI (Copy Control Information) 15が記録される。暗号化タイトルキー14は、暗号化されたタイトルキー情報であり、タイトルキー情報は、タイトル毎に付加される鍵情報である。CCIは、コピーノーマ、コピーワンス、コピーフリー等のコピー制御情報である。

レコーダ2は、デバイスキー21、プロセスMKB22、C2__G23、乱数発生器24、C2__E25、C2__G26およびC2__E CBC27の構成要素を有する。プレーヤ3は、デバイスキー31、プロセスMKB32、C2__G33、C2__D35、C2__G36およびC2__D CBC37の構成要素を有する。

デバイスキー21、31は、個々の装置メーカー、またはアプリケーションソフトウェアベンダー毎に発行された識別番号である。デバイスキーは、ライセンス管理者によって正当な電子機器またはアプリケ
25

ーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報である。DVDメディア1から再生されたMKB12とデバイスキー21とがプロセスMKB22において演算されることによって、リボケーションされたかどうかの判別ができる。レコーダ2におけるのと同様に、プレーヤ3においても、MKB12とデバイスキー31とがプロセスMKB32において演算され、リボケーションされたかどうかの判別がなされる。

さらに、プロセスMKB22、32のそれぞれにおいて、MKB12とデバイスキー21、31からメディアキーが算出される。MKB12の中にレコーダ2またはプレーヤ3のデバイスキーが入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキーを持つレコーダ2またはプレーヤ3が正当なものでないと判断される。すなわち、そのようなレコーダ2またはプレーヤ3がリボケーションされる。

15 C2__G23、33は、それぞれ、メディアキーとメディアIDとを演算し、メディアユニークキーを導出する処理である。

乱数発生器(RNG: Random Number Generator)24は、タイトルキーの生成に利用される。乱数発生器24からのタイトルキーがC2__E25に入力され、タイトルキーがメディアユニークキーで暗号化
20 される。暗号化タイトルキー14がDVDメディア1に記録される。

プレーヤ3では、DVDメディア1から再生された暗号化タイトルキー14とメディアユニークキーとがC2__D35に供給され、暗号化タイトルキーがメディアユニークキーで復号され、タイトルキーが
25 得られる。

レコーダ2においては、CCIとタイトルキーとがC2__G26に

供給され、コンテンツキーが導出される。コンテンツキーがC 2 __ E C B C 2 7に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ 1 3がDVDメディア 1に記録される。

- 5 プレーヤ 3 においては、C C I とタイトルキーとがC 2 __ G 3 6に供給され、コンテンツキーが導出される。コンテンツキーがC 2 __ E C B C 3 7に供給され、DVDメディア 1 から再生された暗号化コンテンツ 1 3 がコンテンツキーを鍵として復号される。

- 第 1 図の構成において、レコーダ 2 による記録の手順について説明
10 する。レコーダ 2 は、DVDメディア 1 からM K B 1 2を読み出し、プロセスM K B 2 2によってデバイスキー 2 1とM K B 1 2とを演算し、メディアキーを計算する。演算結果が予め定められた値を示すならば、デバイスキー 2 1（レコーダ 2 の機器またはアプリケーション）がM K Bによってリボークされたと判定される。レコーダ 2 は、以
15 後の処理を中断し、DVDメディア 1 への記録を禁止する。若し、メディアキーの値が予め定められた値以外であれば、処理を継続する。

- レコーダ 2 は、DVDメディア 1 からメディア I D 1 1を読み、メディアキーと共にメディア I DをC 2 __ G 2 3に入力しメディア毎に
20 異なるメディアユニークキーが演算される。乱数発生器 2 4 で発生させたタイトルキーがC 2 __ E 2 5で暗号化され、暗号化タイトルキー 1 4としてDVDメディア 1 に記録される。タイトルキーとコンテンツのC C I 情報がC 2 __ G 2 6で演算され、コンテンツキーが導出される。コンテンツキーでコンテンツをC 2 __ E C B C 2 7で暗号化し
25 、DVDメディア 1 上に暗号化コンテンツ 1 3としてC C I 1 5と共に記録する。

プレーヤ 3 による再生の手順について説明する。最初に M K B 1 2 を D V D メディア 1 から読み出す。デバイスキー 3 1 と M K B 1 2 を演算し、リボケーションの確認がなされる。デバイスキー 3 1、すなわち、プレーヤ 3 の機器またはアプリケーションがリボークされない

5 場合には、メディア I D を使用してメディアユニークキーが演算され、読み出された暗号化タイトルキー 1 4 とメディアユニークキーからタイトルキーが演算される。タイトルキーと C C I 1 5 とが C 2 __ G 3 6 に入力され、コンテンツキーが導出される。コンテンツキーが C 2 __ D C B C 3 7 に入力され、コンテンツキーを鍵として、D V D メ

10 ディア 1 から再生された暗号化コンテンツ 1 3 に対して C 2 __ D C B C 3 7 の演算が施される。その結果、暗号化コンテンツ 1 3 が復号される。

このように、コンテンツの復号に必要なコンテンツキーを得るためには、D V D メディアの 1 枚毎に異なるメディア I D が必要となるの

15 で、たとえメディア上の暗号化コンテンツが忠実に他のメディアにコピーされても、他のメディアのメディア I D がオリジナルのメディア I D と異なるために、コピーされたコンテンツを復号することができず、コンテンツの著作権を保護することができる。

上述した第 1 図の構成は、記録再生機器として構成されたものである。

20 る。この発明は、D V D メディア 1 に対するコンテンツ保護処理を P C 環境下で扱う場合に適用される。第 2 図を参照して現行の方式による P C とドライブの役割分担を示す。第 2 図において、参照符号 4 が上述した C P R M 規格に準拠した D V D メディア 1 を記録および再生する記録再生装置としての D V D ドライブを示す。

25 参照符号 5 がデータ処理装置としてのホスト例えば P C を示す。ホスト 5 は、D V D メディア 1 に記録可能で、D V D メディア 1 から再

生可能なコンテンツを扱うことができ、且つDVDドライブ4と接続されてデータ交換が可能な装置またはアプリケーションソフトウェアである。例えばPCに対してアプリケーションソフトウェアがインストールされることによってホスト5が構成される。

5 DVDドライブ4とホスト5との間がインターフェース4aで接続されている。インターフェース4aは、ATAPI(AT Attachment with Packet Interface), SCSI(Small Computer System Interface), USB(Universal Serial Bus), IEEE(Institute of Electrical and Electronics Engineers) 1394等である。

10 DVDメディア1には、メディアID11、メディアキープブロック12およびACC(Authentication Control Code)が予め記録されている。ACCは、DVDドライブ4とホスト5との間の認証がDVDメディア1によって異なるようにするために予めDVDメディア1に記録されたデータである。

15 DVDドライブ4は、ACC16をDVDメディア1から読み出す。DVDメディア1から読み出されたACC16がDVDドライブ4のAKE(Authentication and Key Exchange)41に入力されると共に、ホスト5へ転送される。ホスト5は、受け取ったACCをAKE51に入力する。AKE41および51は、乱数データを交換し、この交換した乱数とACCの値とから認証動作の度に異なる値となる共通のセッションキー(バスキーと称する)を生成する。

バスキーがMAC(Message Authentication Code)演算ブロック42および52にそれぞれ供給される。MAC演算ブロック42および52は、AKE41および51でそれぞれ得られたバスキーをパラメータとして、メディアIDおよびメディアキープブロック12のMAC
25 を計算するプロセスである。MKBとメディアIDの完全性(integri

ty) をホスト 5 が確認するために利用される。

MAC 4 2 および 5 2 によってそれぞれ計算された MAC がホスト 5 の比較 5 3 において比較され、両者の値が一致するかどうか判定される。これらの MAC の値が一致すれば、MKB とメディア ID の完全性が確認されたことになる。比較出力でスイッチ SW 1 が制御される。

スイッチ SW 1 は、DVD ドライブ 4 の DVD メディア 1 の記録または再生経路と、ホスト 5 の暗号化／（または）復号モジュール 5 4 との間の信号路を ON／OFF するものとして示されている。スイッチ SW 1 は、信号路の ON／OFF を行うものとして示されているが、より実際には、ON の場合にホスト 5 の処理が継続し、OFF の場合にホスト 5 の処理が停止することを表している。暗号化／復号モジュール 5 4 は、メディアユニークキーと暗号化タイトルキーと CCI とからコンテンツキーを算出し、コンテンツキーを鍵としてコンテンツを暗号化コンテンツ 1 3 へ暗号化し、またはコンテンツキーを鍵として暗号化コンテンツ 1 3 を復号する演算ブロックである。

メディアユニークキー演算ブロック 5 5 は、MKB 1 2 とメディア ID とデバイスキー 5 6 とからメディアユニークキーを演算する演算ブロックである。第 1 図に示すレコーダまたはプレーヤと同様に、デバイスキーと MKB 1 2 とからメディアキーが演算される。メディアキーとメディア ID 1 1 とからメディアユニークキーが演算される。メディアキーが所定の値となった場合には、その電子機器またはアプリケーションソフトウェアが正当なものではないと判断され、リボークされる。したがって、メディアユニークキー演算ブロック 5 5 は、リボケーションを行うリボーク処理部としての機能も有する。

記録時に、比較 5 3 によって完全性が確認された場合には、スイッ

チSW1がONされる。号化／復号モジュール54からスイッチSW1を通じてドライブ4に対して、暗号化コンテンツ13、暗号化タイトルキー14およびCCI15が供給され、DVDメディア1に対してそれぞれ記録される。再生時に、比較53によって完全性が確認された場合には、スイッチSW1がONされる。DVDメディア1からそれぞれ再生された暗号化コンテンツ13、暗号化タイトルキー14およびCCI15がスイッチSW1を通じてホスト5の暗号化／復号モジュール54に対して供給され、暗号化コンテンツが復号される。

10 第3図は、第2図に示す現行のPC環境下のDVDメディアを利用するシステムにおいて、DVDメディア1と、DVDドライブ4と、ホスト5との間の信号の授受の手順を示す。ホスト5がDVDドライブ4に対してコマンドを送り、DVDドライブ4がコマンドに応答した動作を行う。

15 ホスト5からの要求に応じてDVDメディア1上のACCがシークされ、読み出される(ステップS1)。次のステップS2において、読み出されたACCがAKE41に入力されると共に、ホスト5へ転送され、ホスト5では、受け取ったACCがAKE51へ入力される。AKE41および51は、乱数データを交換し、この交換した乱数
20 とACC16の値から認証動作の度に異なる値となるセッションキーとしてのバスキーを生成し、バスキーをDVDドライブ4とホスト5が共有する。相互認証が成立しなかった場合では、処理が中断する。

認証動作は、電源のON後のディスク検出時並びにディスクの交換
25 時には、必ず行われる。記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うよう

にしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

認証が成功すると、ステップ S 3 において、ホスト 5 が DVD ドライブ 4 に対して、DVD メディア 1 からの MKB (メディアキーブロック) パック # 0 の読み出しを要求する。MKB は、パック 0 ~ パック 15 の 16 セクタが 12 回繰り返してリードインエリアに記録されている。パック単位で、エラー訂正符号化がなされている。

DVD ドライブ 4 がステップ S 4 において MKB のパック # 0 を読みに行き、ステップ S 5 において、パック # 0 が読み出される。DVD
10 ドライブ 4 は、モディファイド MKB をホスト 5 へ戻す (ステップ S 6)。MKB を読み出す際に、バスキーをパラメータとして MAC 値を計算し、MKB に対して MAC 値を付加してホスト 5 へデータを転送する。パック # 0 以外の残りの MKB パックの要求と、DVD ドライブ 4 の読み出し動作と、モディファイド MKB パックの転送動作
15 とが MKB のパックがなくなるまで、例えばパック # 15 が読み出され、ホスト 5 へ転送されるまで、ステップ S 7 および S 8 によって繰り返される。

ホスト 5 が DVD ドライブ 4 に対してメディア ID を要求する。DVD
ドライブ 4 が DVD メディア 1 に記録されているメディア ID を
20 読みに行き、ステップ S 11 において、メディア ID が読み出される。DVD ドライブ 4 は、メディア ID を読み出す際に、バスキーをパラメータとしてその MAC 値を計算する。DVD ドライブ 4 はステップ S 12 において、読み出されたメディア ID に対して MAC 値 m1 を付加してホスト 5 へデータを転送する。

25 ホスト 5 では、DVD ドライブ 4 から受け取った MKB 12 およびメディア ID 11 からバスキーをパラメータとして再度 MAC 値を計

算し、計算したMAC値とDVDドライブ4から受け取ったMAC値とを比較53で比較する。両者が一致したならば、正しいMKBおよびメディアIDを受け取ったと判定して、スイッチSW1をONに設定して処理を先に進める。逆に両者が一致しなかったならば、MKB
5 およびメディアIDが改ざんされたものと判定して、スイッチSW1をOFFに設定して処理を中断する。

ステップS13において、ホスト5がDVDドライブ4に対して暗号化コンテンツを要求し、ステップS14において、DVDドライブ4が暗号化コンテンツを読み出し、ステップS13において、読み出
10 した暗号化コンテンツがホスト5に転送される。ホスト5のメディアユニークキー演算ブロック55では、デバイスキー56とMKB12とメディアID11とによってメディアユニークキーが計算される。メディアユニークキーが暗号化／復号モジュール54に供給され、暗号化タイトルキー14、CCI15からコンテンツキーが求められる
15 。コンテンツキーを鍵としてDVDメディア1から読み出された暗号化コンテンツが復号される。DVDメディア1に対して記録されるコンテンツが暗号化される。

第4図のフローチャートにおいて、ステップST1は、MAC演算ブロック42でバスキーをパラメータとして求められたMAC計算値
20 と、MAC演算ブロック53でバスキーをパラメータとして求められたMAC計算値とを比較するステップである。両者が一致すれば、スイッチSW1がステップST2においてONとされる。両者が一致しない場合では、スイッチSW1がステップST3においてOFFとされ、処理が停止する。

25 上述したCPRMでは、DVD-Videoの著作権保護技術であるCSSと同じバスキー生成方法を採用している。CSS認証方式の内容

は、本来秘密であるべき情報であるが、既に解析され一般ユーザーが入手可能なC S Sライセンス管理団体であるDVD-CCA の許諾を得ていないフリーソフトウェアによって動作させることが可能となっている。コンテンツプロテクション処理は、ホスト側でなされる、すなわち

5 、リボケーション判定、メディアキー取得、メディアユニークキー導出、タイトルキー生成・導出からコンテンツキー導出およびコンテンツ暗号化・復号の全てがホスト側の処理であることから、著作権保護技術としての信頼性が低下している。

以下に述べるこの発明は、かかる問題点を解決するものである。一

10 実施形態では、P C環境下でのコンテンツプロテクション処理におけるP Cとドライブの役割分担におけるリボケーション動作とメディアキー導出に関わる情報（ここでは、デバイスキー）をドライブ内部に持ち、P Cとの相互認証を経てセッションキーを導出するものである。

15 第5図は、一実施形態における相互認証の構成を示すブロック図であり、第6図は、ドライブ側の処理の流れを示すフローチャートであり、第7図は、ホスト側の処理の流れを示すフローチャートである。以下の説明において、参照符号101がメディア例えば光ディスクを示し、参照符号102がメディアのドライブを示し、参照符号103

20 がドライブ102とドライブーホストインターフェース104を介して接続されたホストを示す。メディア101は、上述したDVDメディアと同様の情報が予め記録されているものである。メディア101は、記録可能なものに限らず、読み出し専用のもので良い。ホスト103がドライブ102に対して所定のコマンドを送り、その動作を

25 制御する。使用するコマンドは、上述した非特許文献2に記載されているコマンド並びにコマンドを拡張したもの、および、メディア10

1 からコンテンツをセクタ・データとして読み出すための R E A D コマンド、メディア 1 0 1 へコンテンツをセクタ・データとして書き込むための W R I T E コマンドである。

ドライブ 1 0 2 は、ドライブのデバイスキー 1 2 1 を有し、ホスト 5 1 0 3 がホストのデバイスキー 1 3 1 を有している。デバイスキー 1 2 1 は、多くの場合に L S I (Large Scale Integrated Circuit : 大規模集積回路) 内部に配置され、外部から読み出すことができないようセキュアに記憶される。デバイスキー 1 3 1 は、ソフトウェアプログラム内にセキュアに記憶される場合と、ハードウェアとしてセキュアに記憶される場合とがある。ドライブ 1 0 2 がメディア 1 0 1 を扱う正当なドライブとなるためには、一実施形態のように、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成を防止できる効果がある。

15 第 5 図に示すように、ドライブ 1 0 2 には、M K B とデバイスキー 1 2 1 とが入力され、ドライブのデバイスキーがリボケーションされたかどうかを判定するプロセス M K B 1 2 2 が備えられている。ホスト 1 0 3 にも同様に、プロセス M K B 1 3 2 が備えられている。リボケーションされない場合に、プロセス M K B 1 2 2 および 1 3 2 から 20 それぞれメディアキー K m が出力される。リボーク判定処理がなされ、メディアキー K m が得られてから認証処理がなされる。

参照符号 1 2 3、1 2 4 および 1 2 5 は、メディアキー K m をパラメータとして M A C 値を計算する M A C 演算ブロックをそれぞれ示す。また、参照符号 1 2 6、1 2 7 および 1 2 8 は、乱数発生器 (R N 25 G : Random Number Generator) をそれぞれ示す。乱数発生器 1 2 6 が乱数 R a 1 を生成し、乱数発生器 1 2 7 が乱数 R a 2 を生成し、乱数発

生器 1 2 8 が乱数 Ra3 を生成する。乱数発生器 1 2 6、1 2 7、1 2 8 は、例えば L S I の構成の乱数発生器であり、ソフトウェアにより乱数を発生する方法と比較してより真正乱数に近い乱数を発生することができる。乱数発生器を共通のハードウェアとしても良いが、乱数 5 Ra1、Ra2、Ra3 は、互いに独立したものである。

ホスト 1 0 3 に、メディアキー Km をパラメータとして MAC 値を計算する MAC 演算ブロック 1 3 3、1 3 4 および 1 3 5 と、乱数発生器 1 3 6、1 3 7 および 1 3 8 が備えられている。乱数発生器 1 3 6 が乱数 Rb1 を生成し、乱数発生器 1 3 7 が乱数 Rb2 を生成し、乱数 10 発生器 1 3 8 が乱数 Rb3 を生成する。乱数発生器 1 3 6、1 3 7、1 3 8 は、通常はソフトウェアによって乱数を発生するものであるが、ハードウェアによる乱数が利用できる場合にはこれを用いても良い。

ドライブ 1 0 2 において生成された乱数とホスト 1 0 3 において生成された乱数とが交換される。すなわち、乱数 Ra1 および乱数 Rb1 が 15 MAC 演算ブロック 1 2 3 および 1 3 3 に入力され、乱数 Ra2 および乱数 Rb2 が MAC 演算ブロック 1 2 4 および 1 3 4 に入力され、乱数 Ra3 および乱数 Rb3 が MAC 演算ブロック 1 2 5 および 1 3 5 に入力される。

20 ドライブ 1 0 2 の MAC 演算ブロック 1 2 3 が演算した MAC 値と、ホスト 1 0 3 の MAC 演算ブロック 1 3 3 が演算した MAC 値とがホスト 1 0 3 内の比較 1 3 9 において比較され、二つの値が同一か否かが判定される。ここでの MAC 値は、 $eK_m(Ra1 \parallel Rb1)$ と表記される。 $eK_m()$ は、メディアキー Km を鍵として括弧内のデータを暗号 25 化することを表している。Ra1 \parallel Rb1 の記号は、左側に乱数 Ra1 を配し、右側に乱数 Rb1 を配するように、二つの乱数を結合することを表

している。比較の結果、二つの値が同一と判定されると、ホスト 1 0 3 によるドライブ 1 0 2 の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

ホスト 1 0 3 の M A C 演算ブロック 1 3 4 が演算した M A C 値と、
5 ドライブ 1 0 2 の M A C 演算ブロック 1 2 4 が演算した M A C 値とが
ドライブ 1 0 2 内の比較 1 2 9 において比較され、二つの値が同一か
否かが判定される。ここでの M A C 値は、 $eK_m(Rb2 \parallel Ra2)$ と表記され
る。比較の結果、二つの値が同一と判定されると、ドライブ 1 0 2 に
よるホスト 1 0 3 の認証が成功したことになり、そうでない場合には
10 、この認証が失敗したことになる。

かかる相互認証において、比較 1 3 9 および 1 2 9 の両者において
、M A C 値が同一と判定され、ドライブ 1 0 2 およびホスト 1 0 3 の
両者の正当性が確認されると、すなわち、相互認証が成功すると、M
A C 演算ブロック 1 2 5 および 1 3 5 によって、共通のセッションキ
15 ー $eK_m(Ra3 \parallel Rb3)$ がそれぞれ生成される。

さらに、上述した相互認証の処理の流れを第 6 図および第 7 図のフ
ローチャートを参照して説明する。最初に、第 7 図のステップ S T 2
0 において、ホスト 1 0 3 がドライブ 1 0 2 に対して、コマンド R E P O
R T KEYを発行し、M K B の転送を要求する。第 6 図のステップ S T 1
20 0 において、ドライブ 1 0 2 がメディア 1 0 1 から M K B 1 1 2 を読
み出して、ホスト 1 0 3 へ転送する。

次に、ドライブ 1 0 2 がステップ S T 1 1 において、プロセス M K
B 1 2 2 によってメディアキー K_m を計算し、ホスト 1 0 3 がステッ
プ S T 2 1 において、プロセス M K B 1 3 2 によってメディアキー K
25 m を計算する。この計算の過程でそれぞれが内蔵するデバイスキー 1
2 1 および 1 3 1 がリボケーションの対象とされているか否かが自分

自身によって確認される（第6図中のステップST12、第7図中のステップST22）。

ドライブ102およびホスト103のそれぞれは、リボケーションの対象とされている場合にはリボークされ、処理が終了する。若し、
5 ホスト103がリボケーションの対象とされていなければ、ステップST23において、コマンドSEND KEYにより、ドライブ102に対して乱数発生器136および137でそれぞれ生成された乱数Rb1と乱数Rb2を転送する。若し、ドライブ102がリボケーションの対象とされていなければ、ステップST13において、ドライブ102がホ
10 スト103から転送されたこれらの乱数を受け取る。

その後、ホスト103は、コマンドREPORT KEYによりドライブ102に対してドライブ102が持つメディアキーKmを鍵としたMACによるレスポンス値と乱数生成器126が発生した乱数Ra1とをホスト103へ転送することを要求する（ステップST24）。このレス
15 ポンス値は、 $eK_m(Ra1 \parallel Rb1)$ と表記される。 $eK_m()$ は、メディアキーKmを暗号鍵として括弧内のデータを暗号化することを表している。Ra1 \parallel Rb1の記号は、左側に乱数Ra1を配し、右側に乱数Rb1を配するように、二つの乱数を結合することを表している。

ホスト103からコマンドREPORT KEYを受け取ったドライブ102
20 は、ステップST14において、MAC演算ブロック123が生成したMAC値 $eK_m(Ra1 \parallel Rb1)$ と乱数Ra1をホスト103へ転送する。ステップST25において、ホスト103は、自身のMAC演算ブロック133でMAC値を計算し、比較139においてドライブ102から受け取った値と一致するかの確認を行う。若し、受け取ったMAC
25 値と計算されたMAC値とが一致したのなら、ホスト103によるドライブ102の認証が成功したことになる。ステップST25におけ

る比較の結果が同一でない場合には、ホスト 1 0 3 によるドライブ 1 0 2 の認証が失敗したことになり、リジェクト処理がなされる。

ホスト 1 0 3 によるドライブ 1 0 2 の認証が成功した場合には、ステップ S T 2 6 において、ホスト 1 0 3 がドライブ 1 0 2 へコマンド 5 REPORT KEY を送付し、ドライブ 1 0 2 の乱数生成器 1 2 4 および 1 2 5 がそれぞれ生成する乱数 R a 2 と乱数 R a 3 の転送を要求する。このコマンドに応答して、ステップ S T 1 5 において、ドライブ 1 0 2 は、これらの乱数をホスト 1 0 3 へ転送する。

ステップ S T 2 7 において、ホスト 1 0 3 の M A C 演算ブロック 1 0 3 4 は、ドライブ 1 0 2 から受け取った乱数からホスト 1 0 3 が持つメディアキー K m を鍵とした M A C によるレスポンス値 $eK_m(Rb2 \parallel Ra2)$ を計算し、乱数 R b 3 とともに、コマンド SEND KEY を用いてドライブ 1 0 2 へ転送する。

ステップ S T 1 6 において、ドライブ 1 0 2 は、ホスト 1 0 3 から 15 レスポンス値 $eK_m(Rb2 \parallel Ra2)$ および乱数 R b 3 を受け取ると、自身で M A C 値を計算し、ステップ S T 1 7 において、比較 1 2 9 によってホスト 1 0 3 から受け取った M A C 値と一致するかの確認を行う。若し、受け取った M A C 値と計算された M A C 値とが一致したのなら、ドライブ 1 0 2 によるホスト 1 0 3 の認証が成功したことになる。この場合 20 には、ステップ S T 1 8 において、M A C 演算ブロック 1 2 5 がセッションキー $eK_m(Ra3 \parallel Rb3)$ を生成し、また、ホスト 1 0 3 に対して認証が成功したことを示す情報を送信し、認証処理が完了する。セッションキーは、認証動作の度に異なる値となる。

ステップ S T 1 7 における比較の結果が同一でない場合には、ドライブ 25 イブ 1 0 2 によるホスト 1 0 3 の認証が失敗したことになり、ステップ S T 1 9 において、認証が失敗したことを示すエラー情報がホスト

1 0 3 に送信される。

5 ホスト 1 0 3 は、送付したコマンド SEND KEY に対する応答としてドライブ 1 0 2 から認証が成功したか否かを示す情報を受け取り、受け取った情報に基づいてステップ S T 2 8 において、認証完了か否かを
10 判断する。認証が成功したことを示す情報を受け取ることで認証完了と判断し、認証が失敗したことを示す情報を受け取ることで認証が完了しなかったと判断する。認証が完了した場合は、ステップ S T 2 9 において、M A C 演算ブロック 1 3 5 がドライブ側と共通のセッションキー $eK_m(Ra3 \parallel Rb3)$ (例えば 6 4 ビット長) を生成する。認証が完
15 了しなかった場合には、リジェクト処理がなされる。セッションキー $eK_m(Ra3 \parallel Rb3)$ を以下の説明では、適宜 K_s と表記する。

 上述した一実施形態による相互認証は、ドライブ 1 0 2 がリボケーション機能を持つことができ、また、認証専用の特定の認証鍵を必要としない特徴を有している。

15 また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。

 さらに、ドライブ 1 0 2 が比較 1 2 9 によってホスト 1 0 3 の認証結果を確認することで、ドライブ 1 0 2 がホスト 1 0 3 から正規のライセンスを受けた上で実装されたものであるか否かを判定することが
20 可能となる。

 次に、上述した相互認証を行うドライブ 1 0 2 とホスト 1 0 3 とを組み合わせ実現したレコーダの一実施形態の構成を第 8 図に示す。一実施形態のレコーダは、ドライブ 1 0 2 がメディアユニークキーを
25 計算し、計算したメディアユニークキーを相互認証によって生成したセッションキー K_s を用いてセキュアにホスト 1 0 3 に転送する。ま

た、ドライブ 1 0 2 がコンテンツキー導出のための乱数データを生成し、生成した乱数データを相互認証によって生成したセッションキー K_s を用いてホスト 1 0 3 へセキュアに転送し、ホスト 1 0 3 が導出したコンテンツキーを用いてコンテンツを暗号化し、暗号化コンテンツをドライブ 1 0 2 へ転送し、ドライブ 1 0 2 が暗号化コンテンツをメディア 1 0 1 へ記録する構成とされている。

レコーダを構成するドライブ 1 0 2 は、デバイスキー 1 2 1、プロセス MKB 1 2 2、C 2 __G 2 1 4 1、DES (Data Encryption Standard) エンクリプタ 1 4 2、乱数発生器 1 4 3、DES エンクリプタ 1 4 4 の構成要素を有する。

メディア 1 0 1 から再生された MKB 1 1 2 とデバイスキー 1 2 1 とがプロセス MKB 1 2 2 において演算されることによって、リボケーションされたかどうかの判別ができる。プロセス MKB 1 2 2 において、MKB 1 1 2 とデバイスキー 1 2 1 からメディアキーが算出される。MKB 1 1 2 の中にドライブ 1 0 2 のデバイスキー 1 2 1 が入っており、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキー 1 2 1 を持つドライブ 1 0 2 が正当なものでないと判断され、ドライブ 1 0 2 がリボケーションされる。

C 2 __G 1 4 1 は、メディアキーとメディア ID 1 1 1 とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーが DES エンクリプタ 1 4 2 にてセッションキー K_s によって暗号化される。暗号化の方式として、例えば DES CBC モードが使用される。DES エンクリプタ 1 4 2 の出力がホスト 1 0 3 の DES デクリプタ 1 5 1 に送信される。

乱数発生器 1 4 3 によってタイトルキーが生成される。乱数発生器

1 4 3 からのタイトルキーがDESエンクリプタ1 4 4に入力され、
タイトルキーがセッションキーで暗号化される。暗号化タイトルキー
がホスト1 0 3のDESデクリプタ1 5 2に送信される。

5 ホスト1 0 3において、DESデクリプタ1 5 1において、セッシ
ョンキーK_sによってメディアユニークキーが復号される。DESデ
クリプタ1 5 2において、セッションキーK_sによってタイトルキー
が復号される。メディアユニークキーおよびタイトルキーがC 2 __E
1 5 3に供給され、タイトルキーがメディアユニークキーを使用して
C 2 によって暗号化される。暗号化タイトルキー1 1 4がメディア1
10 0 1に記録される。

ホスト1 0 3においては、CCIと復号されたタイトルキーとがC
2 __G 1 5 4に供給され、コンテンツキーが導出される。コンテン
ツキーがC 2 __ECBC 1 5 5に供給され、コンテンツキーを鍵として
コンテンツが暗号化される。暗号化コンテンツ1 1 3がメディア1 0
15 1に記録される。

第9図は、コンテンツ記録時の手順を示すものである。最初に、ホ
スト1 0 3からの要求に応じてメディア1 0 1上のMKBがシークさ
れ、読み出される（ステップS 2 1）。次のステップS 2 2のAKE
(Authentication and Key Exchange)において、上述したようなりボ
20 ーク処理とドライブ1 0 2とホスト1 0 3の相互認証動作がなされる
。

相互認証動作は、電源のON後のディスク検出時並びにディスクの
交換時には、必ず行われる。また、記録ボタンを押して記録動作を行
う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作
25 を行うようにしても良い。一例として、記録ボタンまたは再生ボタン
を押した時に、認証がなされる。

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ 1 0 2 およびホスト 1 0 3 の両者において、セッションキー K_s が生成され、セッションキー K_s が共有される。

- 5 次のステップ S 2 3 において、ホスト 1 0 3 がドライブ 1 0 2 に対してメディアユニークキーを要求する。ドライブ 1 0 2 は、メディア 1 0 1 のメディア ID をシークし（ステップ S 2 4）、メディア ID をメディア 1 0 1 から読み出す（ステップ S 2 5）。ドライブ 1 0 2 は、メディアキーとメディア ID とを演算することによってメディア
- 10 ユニークキーを生成する。ステップ S 2 6 において、メディアユニークキーがセッションキー K_s によって暗号化され、暗号化されたメディアユニークキーがホスト 1 0 3 に転送される。

- 次に、ステップ S 2 7 において、ホスト 1 0 3 がドライブ 1 0 2 に対してタイトルキーを要求する。ステップ S 2 8 において、ドライブ
- 15 1 0 2 がタイトルキーをセッションキー K_s で暗号化し、暗号化したタイトルキーをホスト 1 0 3 に転送する。ホスト 1 0 3 において、セッションキー K_s によって、暗号化されたメディアユニークキーおよび暗号化されたタイトルキーがそれぞれ復号される。

- そして、タイトルキーがメディアユニークキーによって暗号化され
- 20 、暗号化タイトルキーが生成される。また、タイトルキーと C C I からコンテンツキーが生成され、コンテンツキーによってコンテンツが暗号化される。ステップ S 2 9 において、ホスト 1 0 3 からドライブ 1 0 2 に対して、暗号化タイトルキー、暗号化コンテンツおよび C C I が転送される。ステップ S 3 0 において、ドライブ 1 0 2 によって
- 25 、これらの暗号化タイトルキー、暗号化コンテンツおよび C C I がメディア 1 0 1 に対して記録される。

なお、第 8 図のレコーダの構成においては、ドライブ 1 0 2 において乱数発生器 1 4 3 を使用してタイトルキーを生成している。しかしながら、ホスト 1 0 3 に乱数発生器を設け、この乱数発生器によってタイトルキーを生成するようにしても良い。

- 5 次に、上述した相互認証を行うドライブ 1 0 2 とホスト 1 0 3 とを組み合わせせて実現したプレーヤの一実施形態の構成を第 1 0 図に示す。一実施形態のプレーヤは、ドライブ 1 0 2 が計算したメディアユニークキーを相互認証によって生成したセッションキー K_s を用いてセキュアにホスト 1 0 3 に転送し、ホスト 1 0 3 が暗号化タイトルキーをメディアユニークキーによって復号し、タイトルキーと C C I とから導出したコンテンツキーを用いてコンテンツを復号する構成とされている。

プレーヤを構成するドライブ 1 0 2 は、デバイスキー 1 2 1、プロセス M K B 1 2 2、C 2 _ G 2 1 4 1、D E S エンクリプタ 1 4 2 の構成要素を有する。メディア 1 0 1 から再生された M K B 1 1 2 とデバイスキー 1 2 1 とがプロセス M K B 1 2 2 において演算されることによって、リボケーションされたかどうかの判別ができる。プロセス M K B 1 2 2 において、M K B 1 1 2 とデバイスキー 1 2 1 からメディアキーが算出される。

- 20 C 2 _ G 1 4 1 は、メディアキーとメディア I D 1 1 1 とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーが D E S エンクリプタ 1 4 2 にてセッションキー K_s によって暗号化される。暗号化の方式として、例えば D E S C B C モードが使用される。D E S エンクリプタ 1 4 2 の出力がホスト 1 0 3 の D E S デクリプタ 1 5 1 に送信される。

ホスト 1 0 3 において、D E S デクリプタ 1 5 1 において、セッシ

セッションキーK_sによってメディアユニークキーが復号される。メディアユニークキーおよび暗号化タイトルキー114がC2__D153に供給され、暗号化タイトルキーがメディアユニークキーを使用して復号される。復号されたタイトルキーとメディア101から再生されたC5CIがC2__G154に供給され、コンテンツキーが導出される。メディア101から再生された暗号化コンテンツ113がC2デクリプタ155において、コンテンツキーによって復号され、コンテンツが得られる。

- 第11図は、コンテンツ再生時の手順を示すものである。最初に、
- 10 ホスト103からの要求に応じてメディア101上のMKBがシークされ、読み出される（ステップS41）。MKBがパック毎に読み出される。次のステップS42のAKEにおいて、上述したようなリボーク処理とドライブ102とホスト103の相互認証動作がなされる。
- 15 相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ102およびホスト103の両者において、セッションキーK_sが生成され、セッションキーK_sが共有される。

- 次のステップS43において、ホスト103がドライブ102に対してメディアユニークキーを要求する。ドライブ102は、メディア101のメディアIDをシークし（ステップS44）、メディアIDをメディア101から読み出す（ステップS45）。ドライブ102は、メディアキーとメディアIDとを演算することによってメディアユニークキーを生成する。ステップS46において、メディアユニークキーがセッションキーK_sによって暗号化され、暗号化されたメディアユニークキーがホスト103に転送される。
- 20
- 25

次に、ステップS 4 7において、ホスト1 0 3がドライブ1 0 2に対して、暗号化タイトルキー、C C I および暗号化コンテンツを要求する。ステップS 4 8において、ドライブ1 0 2が暗号化タイトルキー1 1 4、C C I 1 1 5 および暗号化コンテンツ1 1 3をメディア1 0 1からリードする。ステップS 4 9において、ドライブ1 0 2が暗号化タイトルキー1 1 4、C C I 1 1 5 および暗号化コンテンツ1 1 3を読み取る。そして、ステップS 5 0において、ドライブ1 0 2が暗号化タイトルキー1 1 4、C C I 1 1 5 および暗号化コンテンツ1 1 3をホスト1 0 3に対して転送する。

- 10 ホスト1 0 3において、タイトルキーが復号され、タイトルキーとC C I とからコンテンツキーが求められ、コンテンツキーを鍵として暗号化コンテンツが復号される。

第1 0 図に示すプレーヤの構成においては、ホスト1 0 3が暗号化タイトルキーを復号するデクリプタC 2 __D 1 5 3を備えているが、
15 ドライブ1 0 2が暗号化タイトルキーを復号するデクリプタを備えるようにしても良い。この場合、復号されたタイトルキーがホスト1 0 3のコンテンツキー生成用のC 2 __G 1 5 4に対してセキュアに転送される。または、ドライブ1 0 2にコンテンツキー生成装置C 2 __G
20 を設け、ドライブ1 0 2において復号されたタイトルキーとC C I とからコンテンツキーを生成するようにしても良い。この場合、復号されたコンテンツキーがホスト1 0 3のC 2 __D C B C 1 5 5へセキュアに転送される。

第1 2 図は、相互認証を行うドライブ1 0 2とホスト1 0 3とを組み合わせ実現したレコーダの他の実施形態の構成を示す。他の実施
25 形態のレコーダは、ドライブ1 0 2が計算したメディアユニークキーを相互認証によって生成したセッションキーK sを用いてセキュアに

5 ホスト 1 0 3 に転送する。また、ドライブ 1 0 2 においてコンテンツ
キーが生成され、生成されたコンテンツキーがセッションキー K_s を
用いてホスト 1 0 3 へセキュアに転送され、ホスト 1 0 3 が復号した
コンテンツキーを用いてコンテンツを暗号化し、暗号化コンテンツを
ドライブ 1 0 2 へ転送し、ドライブ 1 0 2 が暗号化コンテンツをメ
ディア 1 0 1 へ記録する構成とされている。すなわち、第 8 図に示す上
述したレコーダでは、ホスト 1 0 3 においてコンテンツキーを生成し
たが、他の実施形態では、ドライブ 1 0 2 において、コンテンツキー
を生成している。

- 10 第 1 2 図に示すように、メディア 1 0 1 から再生された $MKB\ 1\ 1$
2 とデバイスキー 1 2 1 とがプロセス $MKB\ 1\ 2\ 2$ において演算され
ることによって、メディアキーが算出され、 $C2_G\ 1\ 4\ 1$ において
、メディアキーとメディア $ID\ 1\ 1\ 1$ とが演算し、メディアユニーク
キーが導出される。メディアユニークキーが DES エンクリプタ 1 4
15 2 にてセッションキー K_s によって暗号化され、 DES エンクリプタ
1 4 2 の出力がホスト 1 0 3 の DES デクリプタ 1 5 1 に送信され、
 DES デクリプタ 1 5 1 によってメディアユニークキーが導出される
。

20 さらに、ドライブ 1 0 2 の乱数発生器 1 4 3 によってタイトルキー
が生成され、乱数発生器 1 4 3 からのタイトルキーがホスト 1 0 3 の
 $C2_E\ 1\ 5\ 3$ に供給され、タイトルキーがメディアユニークキーを
使用して $C2$ によって暗号化される。暗号化タイトルキー 1 1 4 がメ
ディア 1 0 1 に記録される。

25 ホスト 1 0 3 において、セッションキー K_s を鍵として MAC 演算
ブロック 1 5 8 により CCI の MAC 値 $eK_s\ (CCI)$ が計算され
、 CCI とともにドライブ 1 0 2 へ転送される。

ドライブ 102 において、ホスト 103 から受け取った CCI からセッションキー Ks を鍵として MAC 演算ブロック 157 により CCI の MAC 値 eKs (CCI) が計算され、ホスト 103 から受け取った MAC 値とともに比較 159 へ供給される。

- 5 比較 159 では、両方の MAC 値が一致したならば、ホスト 103 から受け取った CCI の改ざんは無いものと判断し、スイッチ SW2 を ON する。一致しなかった場合は、CCI は改ざんされたものとみなし、スイッチ SW2 を OFF し、以降の処理を中断する。

ドライブ 102 において、ホスト 103 から受け取った CCI とタイトルキーとが C2__G145 に供給され、コンテンツキーが導出される。コンテンツキーが DES エンクリプタ 146 に供給され、セッションキー Ks を鍵として、コンテンツキーが暗号化される。暗号化コンテンツキーがホスト 103 の DES デクリプタ 156 に転送される。

- 15 DES デクリプタ 156 でセッションキー Ks を鍵として復号されたコンテンツキーが C2__ECBC155 に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ 113 がドライブ 102 に転送され、ドライブ 102 によってメディア 101 に記録される。

- 20 なお、第 12 図に示すレコーダにおいては、タイトルキーがドライブ 102 の乱数発生器 143 によって生成されている。しかしながら、ホスト 103 側に乱数発生器を設け、この乱数発生器によってタイトルキーを生成しても良い。この場合には、生成されたタイトルキーがホスト 103 からドライブ 102 のコンテンツキー生成のための C
- 25 2__G145 に対して転送される。

第 13 図は、レコーダの他の実施形態によるコンテンツ記録時の手

順を示すものである。最初に、ホスト 1 0 3 からの要求に応じてメディア 1 0 1 上の MKB がシークされ、読み出される（ステップ S 6 1）。次のステップ S 6 2 の AKE において、リボーク処理とドライブ 1 0 2 とホスト 1 0 3 の相互認証動作がなされる。

- 5 相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ 1 0 2 およびホスト 1 0 3 の両者において、セッションキー K_s が生成され、セッションキー K_s が共有される。

- 次のステップ S 6 3 において、ホスト 1 0 3 がドライブ 1 0 2 に対してメディアユニークキーを要求する。ドライブ 1 0 2 は、メディア 1 0 1 のメディア ID をシークし（ステップ S 6 4）、メディア ID をメディア 1 0 1 から読み出す（ステップ S 6 5）。ドライブ 1 0 2 は、メディアキーとメディア ID とを演算することによってメディアユニークキーを生成する。ステップ S 6 6 において、メディアユニークキーがセッションキー K_s によって暗号化され、暗号化されたメディアユニークキーがホスト 1 0 3 に転送される。

- 次に、ステップ S 6 7 において、ホスト 1 0 3 がドライブ 1 0 2 に対してタイトルキーを要求する。ステップ S 6 8 において、ドライブ 1 0 2 がタイトルキーをホスト 1 0 3 に転送する。ホスト 1 0 3 において、セッションキー K_s によって、暗号化されたメディアユニークキーが復号される。そして、タイトルキーがメディアユニークキーによって暗号化され、暗号化タイトルキーが生成される。

- また、ステップ S 6 9 において、ホスト 1 0 3 がドライブ 1 0 2 に対して CCI を送る。このとき、CCI の改ざんを回避するために CCI の認証データとして計算された MAC 値 $e K_s (CCI)$ を付加して転送する。ドライブ 1 0 2 において、CCI の改ざんが無いこと

を確認後、タイトルキーとCCIからコンテンツキーが生成され、コンテンツキーがセッションキーKsで暗号化される。ステップS70において、ホスト103がドライブ102に対してコンテンツキーを要求すると、ステップS71において、ドライブ102が暗号化されたコンテンツキーをホスト103に送る。

ホスト103は、暗号化コンテンツキーをセッションキーKsによって復号し、コンテンツキーを得る。コンテンツキーによってコンテンツが暗号化される。ステップS72において、ホスト103からドライブ102に対して、暗号化タイトルキー、暗号化コンテンツおよびCCIが転送される。ステップS73において、ドライブ102によって、暗号化タイトルキー、暗号化コンテンツおよびCCIがメディア101に対して記録される。

上述した第12図に示す構成のレコーダは、ドライブ102において、真正乱数またはそれに近い乱数をハードウェア例えばLSIによって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。また、ドライブ102において、ハードウェア構成によってコンテンツキーを生成するので、著作権保護の実装を強力とすることができる。

この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばタイトルキーは、タイトル毎のキーであるが、この発明では、乱数情報であれば、タイトル毎に異なることは、必要ではない。

また、上述した説明においては、著作権保護技術としてCPRMおよびCPRMを拡張した例を挙げたが、CPRM以外の著作権保護技術に対してもこの発明を適用することができる。例えば、特開2001-

352322号公報において提案されるツリー構造の鍵配布構成に基づく著作権保護技術に対して適用可能である。また、P C ベースのシステムに対してこの発明が適用されるが、このことは、P C とドライブを組み合わせる構成にのみ限定されることを意味するものではない。例えば
5 携帯型動画または静止画カメラの場合に、メディアとして光ディスクを使用し、メディアを駆動するドライブとドライブを制御するマイクロコンピュータが設けられる動画または静止画カメラシステムに対してもこの発明を適用することが可能である。

この発明では、メディア上に記録された鍵情報（M K B）と各デバイスまたは各アプリケーションに記憶されている鍵情報（デバイスキー）から同一の値として導かれる鍵情報（メディアキー）を利用して相互認証がなされる。したがって、この発明においては、認証のためだけに用意される特定の認証鍵を必要とせず、秘密情報を少なくでき、また、デバイスまたはアプリケーションによってデバイスキーを異
10 ならせることが可能であるので、秘密情報が不正に読み取られる危険性を少なくできる。

この発明では、著作権保護技術に関する秘密情報である電子機器またはアプリケーションソフトウェア固有の情報例えばデバイスキーがドライブ内に実装されているので、情報処理装置にインストールされ
20 るアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持たせることが容易に実施でき、また、ディスクからのデータとしてそのまま読み出された暗号化コンテンツが「D e C S S」のような解読ソフトウェアにより
25 り復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を防ぐことができること

から、著作権保護技術の安全性を確保することができる。

また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。

- 5 さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばL S Iによって生成できるので、P C内でソフトウェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少な
- 10 くできる。

請 求 の 範 囲

1. 不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法において、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第1の判定ステップを有し、

- 10 上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定ステップを有し、

- 上記第1の判定ステップによって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、上記第2の判定ステップによって無効化すべきという判定をされなかった場合に生成される第2の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法。
- 15

2. 請求の範囲第1項において、

- 20 上記相互認証ステップは、

上記情報処理装置が上記伝達手段を介して正常に動作しているかを上記再生装置において確認する第1の確認ステップと、

- 上記再生装置が上記伝達手段を介して正常に動作しているかを上記情報処理装置において確認する第2の確認ステップとを有することを特徴とする請求の範囲第1項に記載の相互認証方法。
- 25

3. 請求の範囲第2項において、

上記再生装置は、

乱数を生成する第 1 の乱数生成ステップと、

所定の計算をする第 1 の計算ステップとを有し、

上記情報処理装置は、

5 乱数を生成する第 2 の乱数生成ステップと、

所定の計算をする第 2 の計算ステップとを有し、

上記第 1 の確認ステップは、

上記第 1 の乱数生成ステップにより生成される第 1 の乱数と、上記

第 2 の乱数生成ステップにより生成される第 2 の乱数とを上記伝達手

10 段を介して上記再生装置と上記情報処理装置との間で相互に交換する

第 1 の乱数交換ステップと、

上記再生装置において、少なくとも上記第 1 の鍵情報と上記相互に

交換された第 1 の乱数および第 2 の乱数とを用いて上記第 1 の計算ス

テップにより計算した結果と、上記情報処理装置から上記伝達手段を

15 介して送られた、少なくとも上記第 2 の鍵情報と上記相互に交換され

た第 1 の乱数および第 2 の乱数とを用いて上記第 2 の計算ステップに

より計算した結果とが同一であることを比較する第 1 の比較ステップと

を有し、

上記第 2 の確認ステップは、

20 上記第 1 の乱数生成ステップにより生成される第 3 の乱数と、上記

第 2 の乱数生成ステップにより生成される第 4 の乱数とを上記伝達手

段を介して上記再生装置および上記情報処理装置との間で相互に交換

する第 2 の乱数交換ステップと、

上記情報処理装置において、上記再生装置から上記伝達手段を介し

25 て送られた、少なくとも上記第 1 の鍵情報と上記相互に交換された第

3 の乱数および第 4 の乱数とを用いて上記第 1 の計算ステップにより

計算した結果と、少なくとも上記第 2 の鍵情報と上記相互に交換された第 3 の乱数および第 4 の乱数とを用いて上記第 2 の計算ステップにより計算した結果とが同一であることを比較する第 2 の比較ステップとを有していることを特徴とする相互認証方法。

- 5 4. 不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムであって、

- 10 上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第 1 の判定ステップを有し、

- 上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第 2 の判定ステップを有し、
- 15 上記第 1 の判定ステップによって無効化すべきという判定をされなかった場合に生成される第 1 の鍵情報と、上記第 2 の判定ステップによって無効化すべきという判定をされなかった場合に生成される第 2 の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認

- 20 証する相互認証ステップとを有することを特徴とする相互認証方法のプログラム。

5. 不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムを格納した記録媒体であって、
- 25

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第1の判定ステップを有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定ステップを有し、

上記第1の判定ステップによって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、上記第2の判定ステップによって無効化すべきという判定をされなかった場合に生成される第2の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプログラムを格納した記録媒体。

6. 不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置とを備える信号処理システムであって、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第1の判定手段を有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定手段を有し、

上記第1の判定手段によって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、上記第2の判定手段によって無効化すべきという判定をされなかった場合に生成される第2の鍵情報

とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証手段と、

上記相互認証手段による相互認証後に、上記再生装置および上記情報処理装置に共通の共通鍵を生成する共通鍵生成手段とを備えること

5 を特徴とする信号処理システム。

7. 請求の範囲第6項において、

上記相互認証手段は、

上記情報処理装置が上記伝達手段を介して正常に動作しているかを上記再生装置において確認する第1の確認手段と、

10 上記再生装置が上記伝達手段を介して正常に動作しているかを上記情報処理装置において確認する第2の確認手段とを有することを特徴とする信号処理システム。

8. 請求の範囲第7項において、

上記再生装置は、

15 乱数を生成する第1の乱数生成手段と、
所定の計算をする第1の計算手段とを有し、
上記情報処理装置は、

乱数を生成する第2の乱数生成手段と、
所定の計算をする第2の計算手段とを有し、

20 上記第1の確認手段は、

上記第1の乱数生成手段により生成される第1の乱数と、上記第2の乱数生成手段により生成される第2の乱数とを上記伝達手段を介して上記再生装置と上記情報処理装置との間で相互に交換する第1の乱数交換手段と、

25 上記再生装置において、少なくとも上記第1の鍵情報と上記相互に交換された第1の乱数および第2の乱数とを用いて上記第1の計算手

段により計算した結果と、上記情報処理装置から上記伝達手段を介して送られた、少なくとも上記第 2 の鍵情報と上記相互に交換された第 1 の乱数および第 2 の乱数とを用いて上記第 2 の計算手段により計算した結果とが同一であるかを比較する第 1 の比較手段とを有し、

5 上記第 2 の確認手段は、

 上記第 1 の乱数生成手段により生成される第 3 の乱数と、上記第 2 の乱数生成手段により生成される第 4 の乱数とを上記伝達手段を介して上記再生装置および上記情報処理装置との間で相互に交換する第 2 の乱数交換手段と、

10 上記情報処理装置において、上記再生装置から上記伝達手段を介して送られた、少なくとも上記第 1 の鍵情報と上記相互に交換された第 3 の乱数および第 4 の乱数とを用いて上記第 1 の計算手段により計算した結果と、少なくとも上記第 2 の鍵情報と上記相互に交換された第 3 の乱数および第 4 の乱数とを用いて上記第 2 の計算手段により計算した結果とが同一であるかを比較する第 2 の比較手段とを有していることを特徴とする信号処理システム。

9. 請求の範囲第 8 項において、

 上記共通鍵生成手段は、

20 上記第 1 の乱数生成手段により生成される第 5 の乱数と、上記第 2 の乱数生成手段により生成される第 6 の乱数とを上記伝達手段を介して上記再生装置と上記情報処理装置との間で相互に交換する第 3 の乱数交換手段と、

 上記再生装置において、少なくとも上記第 1 の鍵情報と上記第 5 の乱数と上記第 6 の乱数とを用いて上記共通鍵を生成する第 1 の共通鍵生成手段と、

 上記情報処理装置において、少なくとも上記第 2 の鍵情報と上記第

5 の乱数と上記第 6 の乱数とを用いて上記共通鍵を生成する第 2 の共通鍵生成手段とを有することを特徴とする信号処理システム。

10 請求の範囲第 9 項において、

上記伝達手段を介して、上記共通鍵を用いた共通鍵暗号方式で上記
5 再生装置から上記情報処理装置へ情報を送る第 1 の送信手段と、

上記再生装置において、上記第 1 の鍵情報と上記記録媒体固有の情報を
用いて記録媒体固有の鍵情報を生成する中間鍵情報生成手段とを
備えることを特徴とする請求の範囲第 7 項に記載の信号処理システム
。

10 11 請求の範囲第 10 項において、

第 3 の鍵情報を、少なくとも上記記録媒体固有の鍵情報を用いて暗
号化する鍵情報暗号化手段と、

上記鍵情報暗号化手段により暗号化された上記第 3 の鍵情報を上記
記録媒体に記録する暗号化鍵情報記録手段と、

15 上記第 3 の鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最
終暗号化鍵生成手段と、

上記コンテンツ情報暗号化鍵を用いて暗号化されたコンテンツ情報を
上記記録媒体に記録するコンテンツ情報記録手段とを備えることを
特徴とする信号処理システム。

20 12 請求の範囲第 11 項において、

上記鍵情報暗号化手段、上記暗号化鍵情報記録手段、上記最終暗号
化鍵生成手段、上記コンテンツ情報記録手段は、

上記情報処理装置が有しているとともに、

上記記録媒体固有の鍵情報は、

25 上記第 1 の送信手段により上記情報処理装置へ送られることを特徴
とする信号処理システム。

- 1 3 . 請求の範囲第 1 2 項において、
上記第 3 の鍵情報は、
上記再生装置において前期第 1 の乱数生成手段により生成された第
7 の乱数に基づいた鍵情報であるとともに、
- 5 当該第 3 の鍵情報は、
上記第 1 の送信手段により上記情報処理装置に送られることを特徴
とする信号処理システム。
- 1 4 . 請求の範囲第 1 2 項において、
上記第 3 の鍵情報は、
- 10 上記情報処理装置において上記第 2 の乱数生成手段により生成され
た第 8 の乱数に基づいた鍵情報であることを特徴とする信号処理シス
テム。
- 1 5 . 請求の範囲第 1 1 項において、
上記鍵情報暗号化手段、上記暗号化鍵情報記録手段、上記コンテン
ツ情報記録手段は、
- 15 上記情報処理装置が有しており、
上記記録媒体固有の鍵情報は、
上記第 1 の送信手段により上記情報処理装置へ送られるとともに、
- 20 上記最終暗号化鍵生成手段は、
上記再生装置が有しており、
上記最終暗号化鍵生成手段により生成された上記コンテンツ情報暗
号化鍵は、
上記第 1 の送信手段により上記情報処理装置へ送られることを特徴
とする信号処理システム。
- 25 1 6 . 請求の範囲第 1 5 項において、

上記第 3 の鍵情報は、

上記再生装置において上記第 1 の乱数生成手段により生成された第 9 の乱数を基にした鍵情報であることを特徴とする請求の範囲第 1 3 項に記載の信号処理システム。

5 17. 請求の範囲第 1 5 項において、

上記第 3 の鍵情報は、

上記情報処理装置において上記第 2 の乱数生成手段により生成された第 1 0 の乱数を基にした鍵情報であるとともに、

10 上記伝達手段を介して、上記共通鍵を用いた共通鍵暗号方式で上記情報処理装置から上記再生装置へ情報を送る第 2 の送信手段により上記再生装置の上記最終暗号化鍵生成手段に送られることを特徴とする信号処理システム。

18. 請求の範囲第 1 0 項において、

15 上記記録媒体から読み出される暗号化された第 4 の鍵情報を、少なくとも上記記録媒体固有の鍵情報を用いて復号する鍵情報復号手段と、

上記第 4 の鍵情報に基づいてコンテンツ情報復号鍵を生成する最終復号鍵生成手段と、

20 上記コンテンツ情報復号鍵を用いて上記コンテンツ情報を復号するコンテンツ情報復号手段とを備えていることを特徴とする信号処理システム。

19. 請求の範囲第 1 8 項において、

上記最終復号鍵生成手段、上記コンテンツ情報復号手段は、

25 上記情報処理装置が有していることを特徴とする信号処理システム。

20. 請求の範囲第 1 9 項において、

- 上記鍵情報復号手段は、
上記情報処理装置が有しており、
上記記録媒体固有の鍵情報は、
上記第 1 の送信手段によって上記情報処理装置へ送られることを特
- 5 徴とする信号処理システム。
- 2 1 . 請求の範囲第 1 9 項において、
上記鍵情報復号手段は、
上記再生装置が有しており、
復号された上記第 4 の鍵情報は、
- 10 上記第 1 の送信手段によって上記情報処理装置へ送られることを特
徴とする信号処理システム。
- 2 2 . 請求の範囲第 1 8 項において、
上記最終復号鍵生成手段は、
上記再生装置が有していることを特徴とする信号処理システム。
- 15 2 3 . 請求の範囲第 2 2 項において、
上記鍵情報復号手段は、
上記再生装置が有しており、
上記再生装置において生成された上記コンテンツ情報復号鍵は、
上記第 1 の送信手段によって上記情報処理装置へ送られることを特
- 20 徴とする信号処理システム。
- 2 4 . 不正な電子機器を判別するためのリボケーション情報記録媒体
固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す
再生部を有し、上記コンテンツ情報が伝達手段を介して情報処理装置
に送信され、処理される信号処理システムにおける再生装置であって
- 25 、
当該再生装置を表す情報と上記リボケーション情報とを用いて当該

再生装置を無効化すべきか否かを判定する第 1 の判定手段を有し、

上記第 1 の判定手段によって無効化すべきという判定をされなかった場合に生成される第 1 の鍵情報と、

- 上記情報処理装置に設けられている当該情報処理装置を表す情報と
- 5 上記リボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第 2 の判定手段によって無効化すべきという判定をされなかった場合に生成される第 2 の鍵情報とを用いて、上記情報処理装置と相互に認証する相互認証手段と、

- 上記相互認証手段による相互認証後に、上記情報処理装置と共通の
- 10 共通鍵を生成する共通鍵生成手段とを備えることを特徴とする再生装置。

- 2 5 . 不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、再生装置がコンテンツ情報を読み出し、上記コンテンツ情報が伝達手段を介して受信され、処
- 15 理される情報処理装置であって、

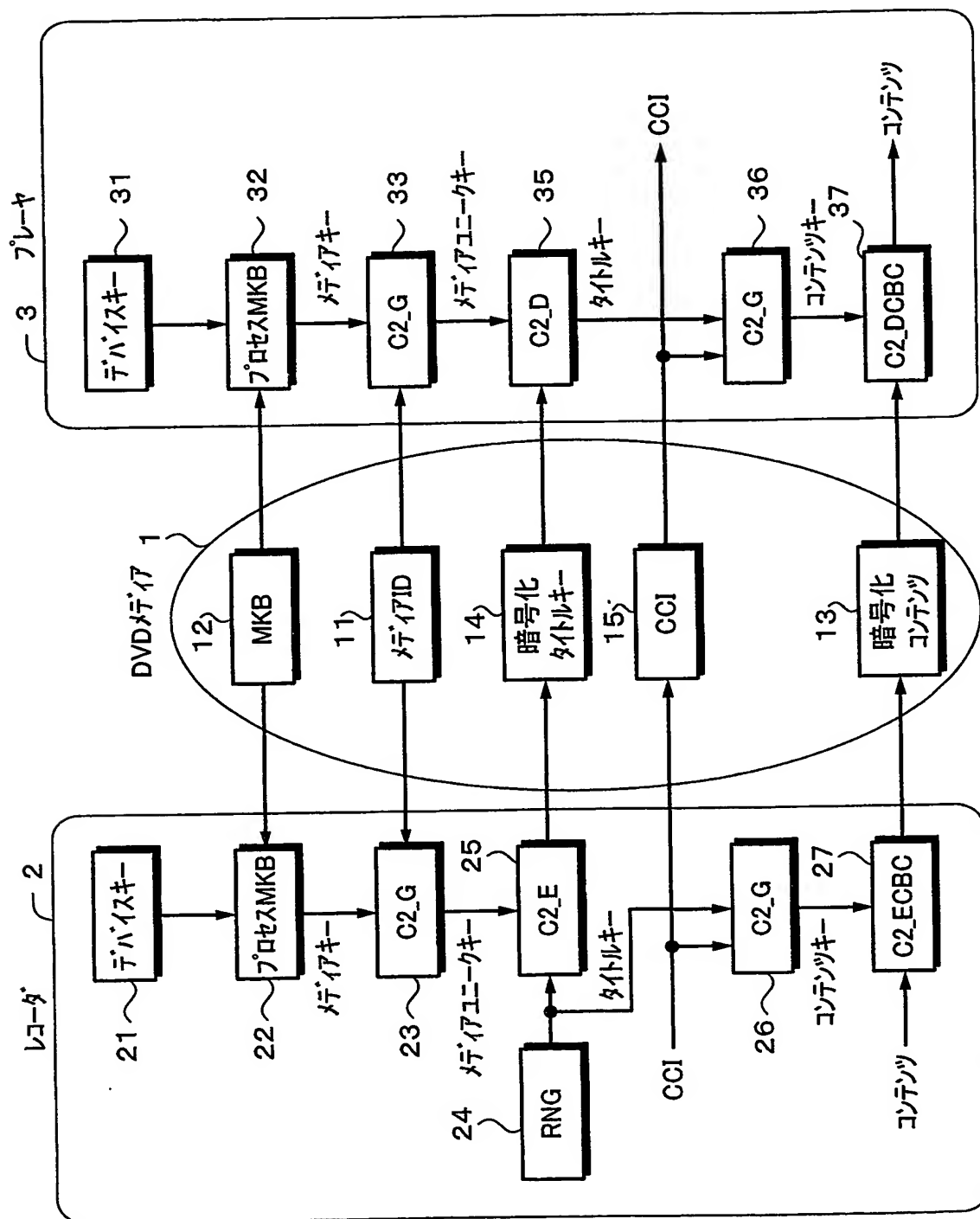
- 上記再生装置に設けられている第 1 の判定手段によって、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定し、上記第 1 の判定手段によって無効化すべきという判定をされなかった場合に生成される第 1 の鍵情報と、
- 20 当該情報処理装置を表す情報と上記リボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第 2 の判定手段を有し、

- 上記第 1 の鍵情報と、上記第 2 の判定手段によって無効化すべきという判定をされなかった場合に生成される第 2 の鍵情報とを用いて、
- 25 上記再生装置と相互に認証する相互認証手段と、

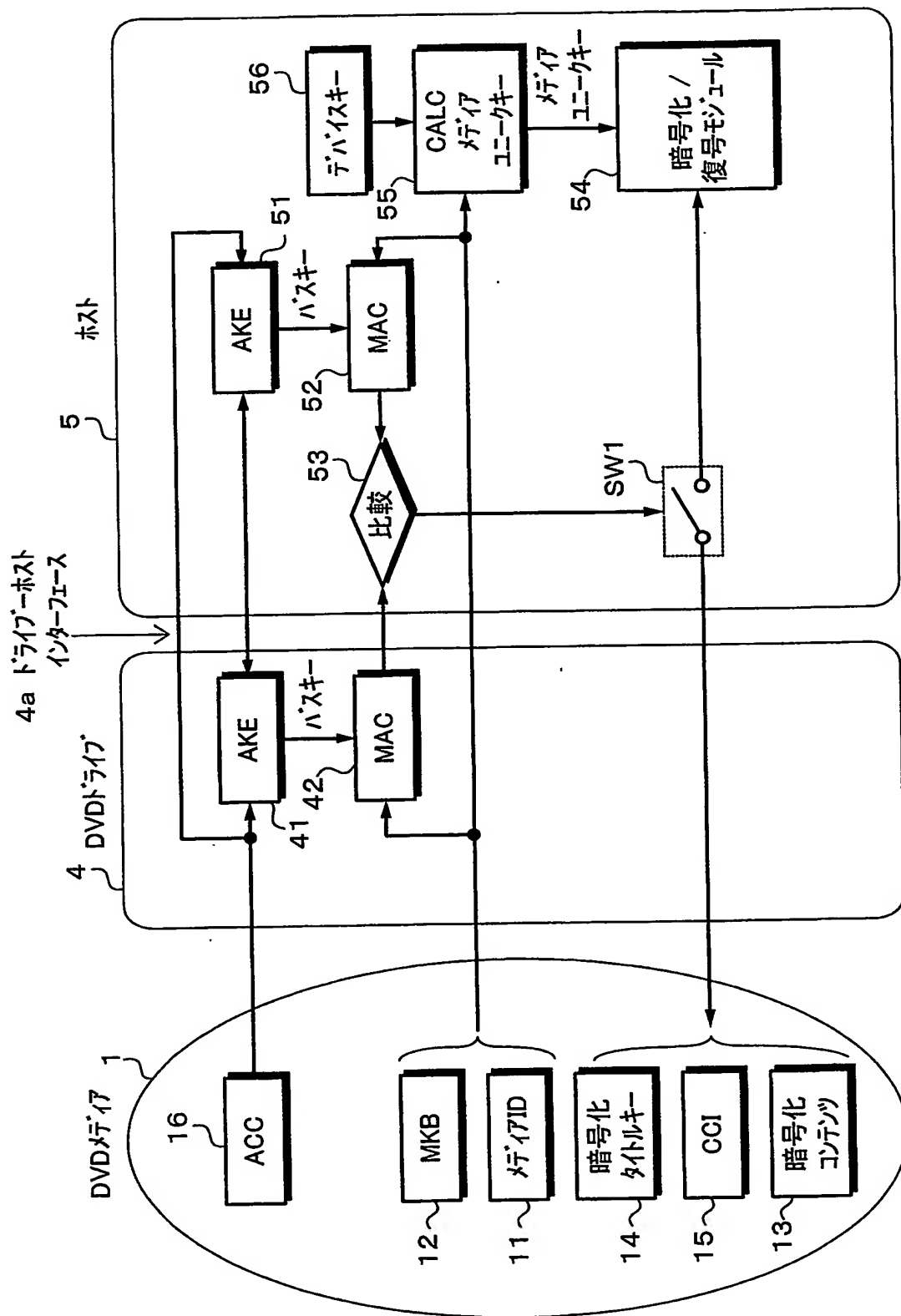
上記相互認証手段による相互認証後に、上記再生装置と共通の共通

鍵を生成する共通鍵生成手段とを備えることを特徴とする情報処理装置。

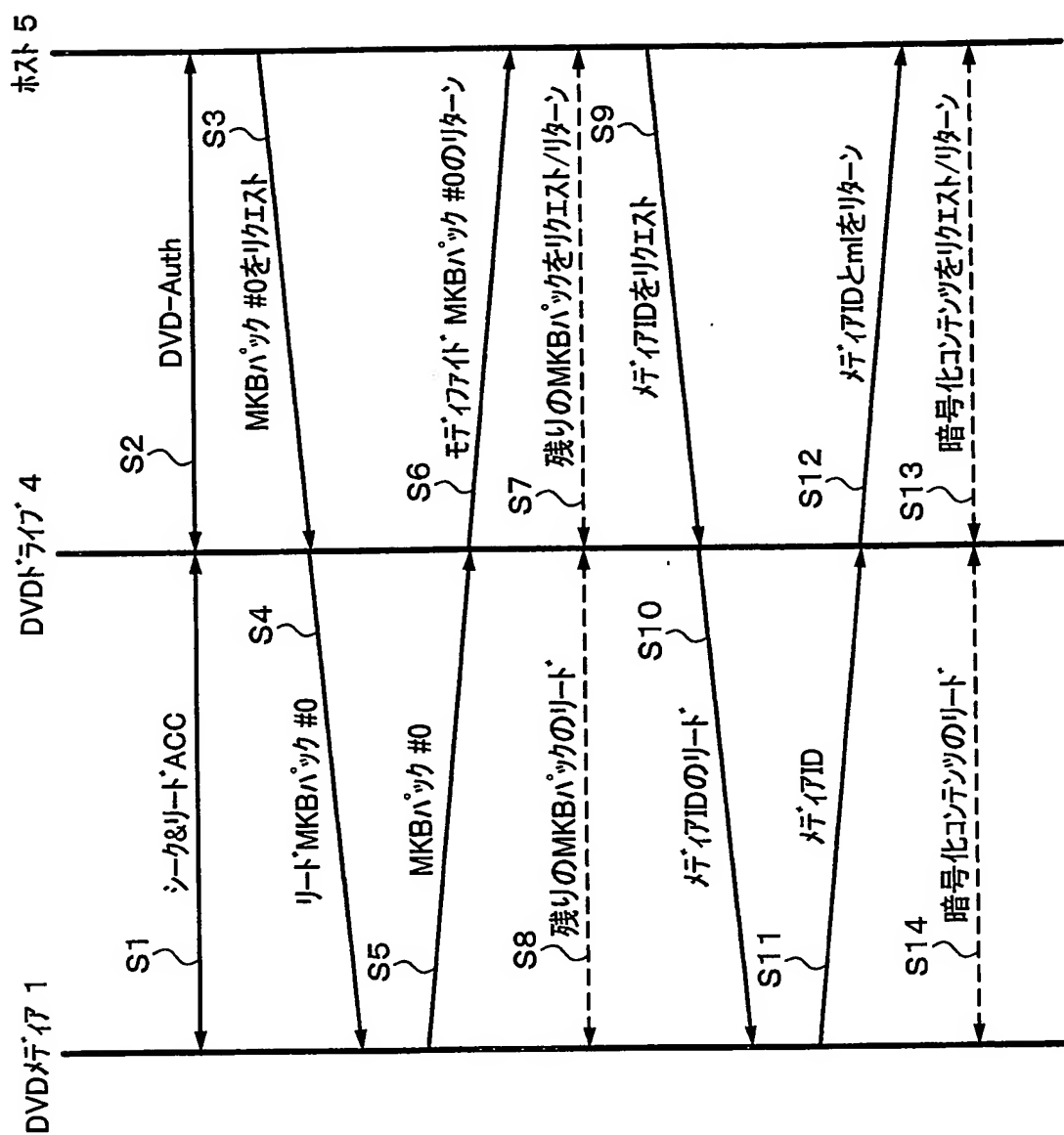
第1図



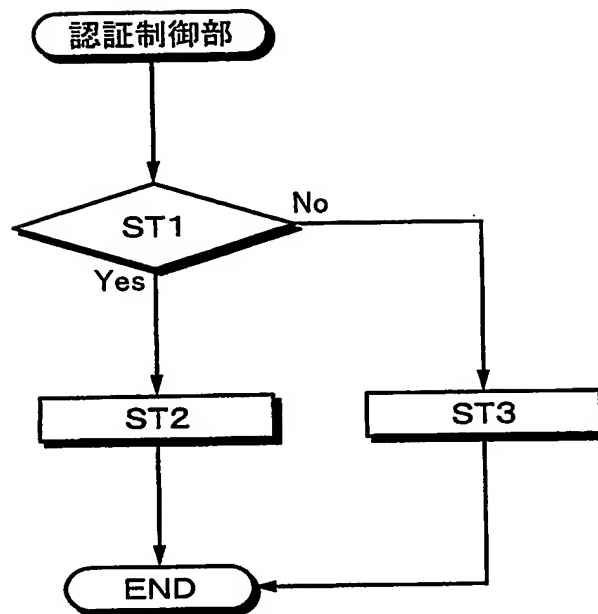
第2図



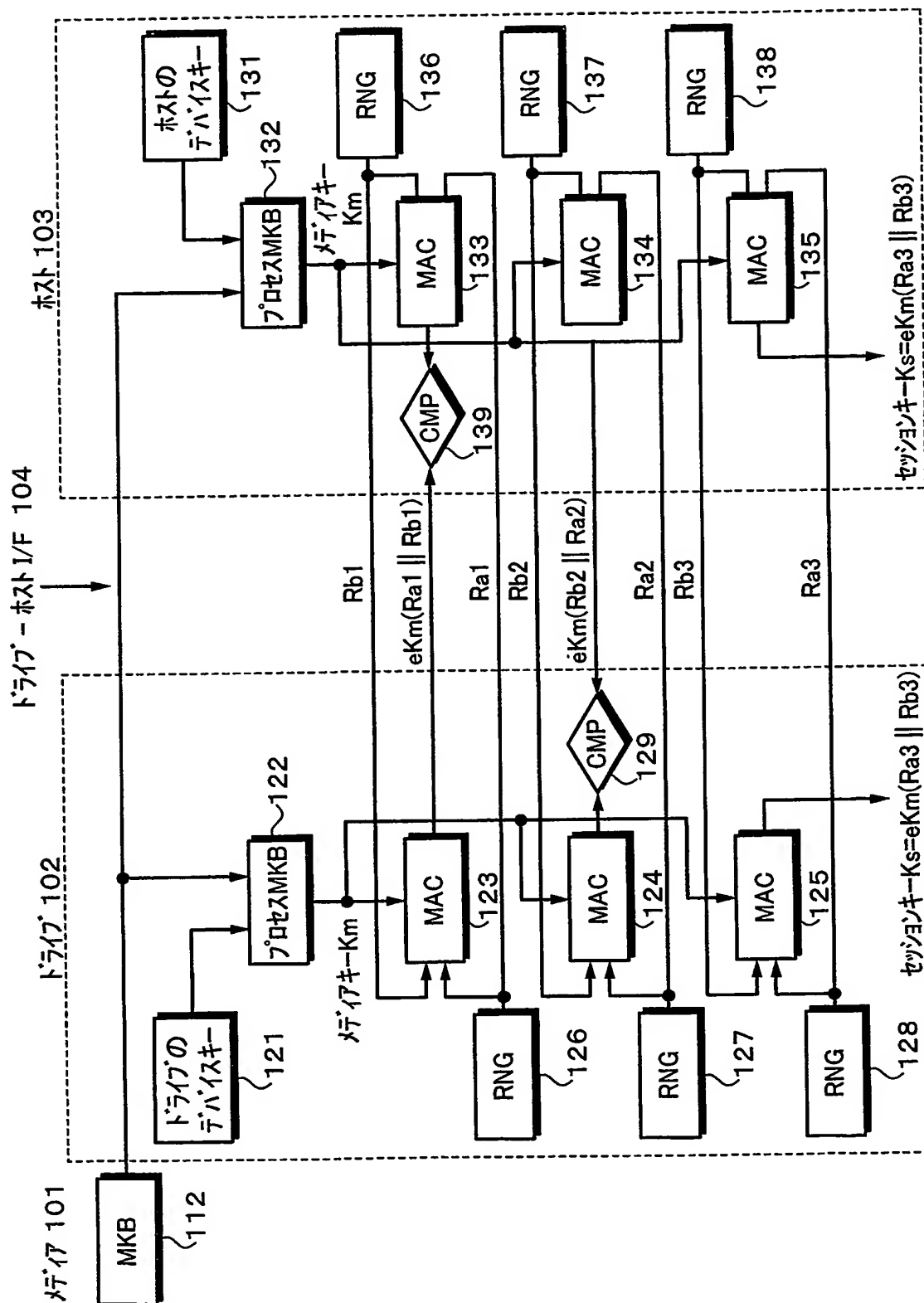
第3図



第4図

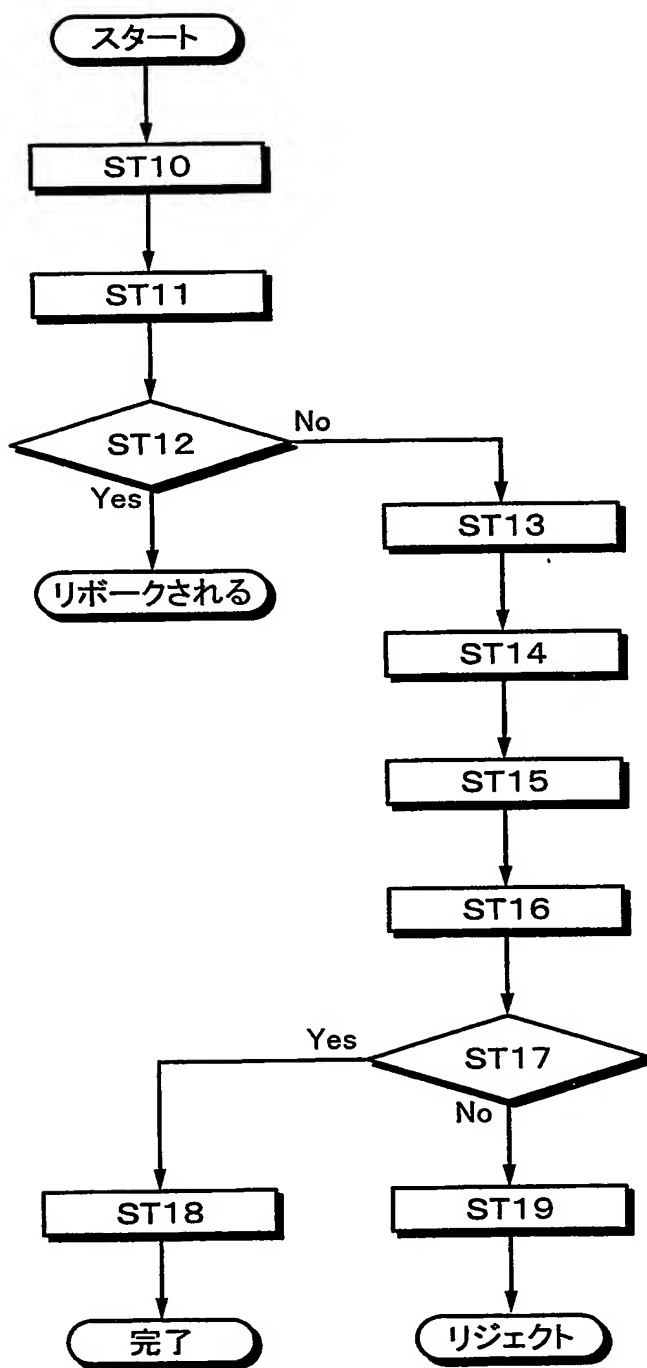


第5図

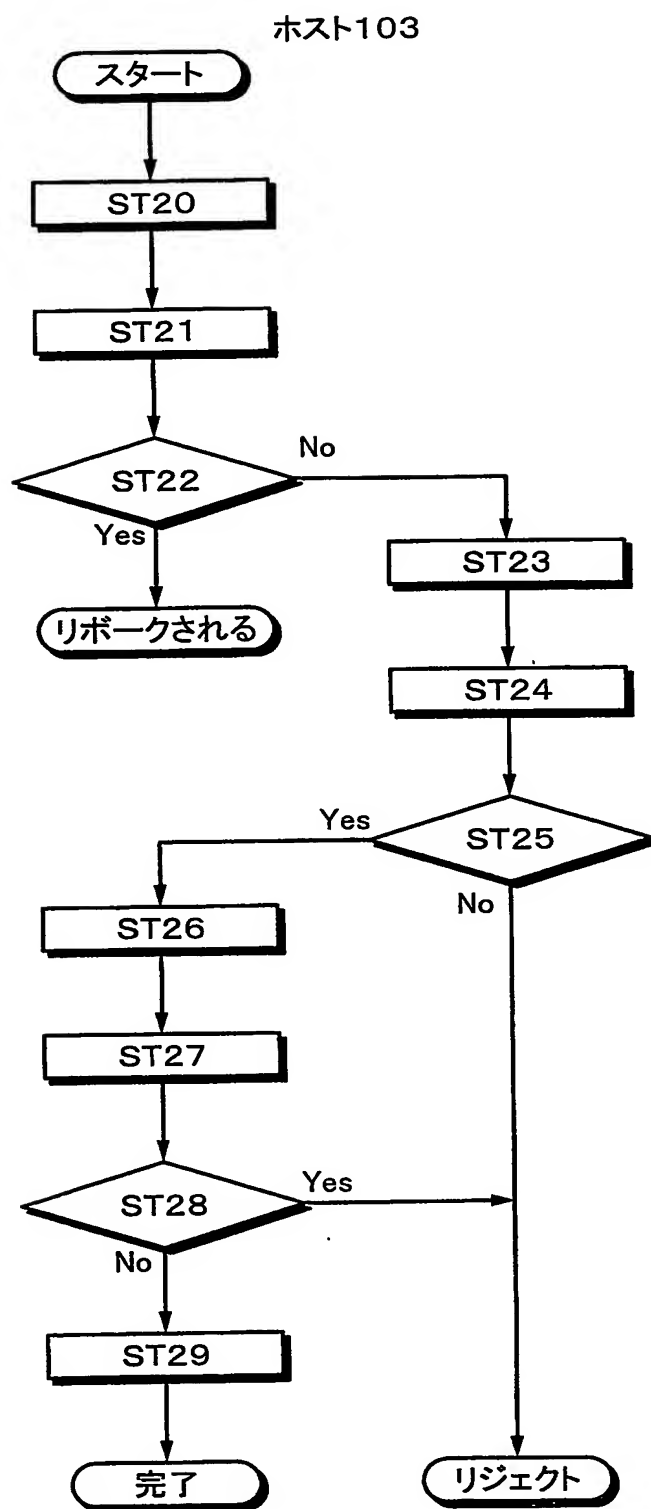


第6図

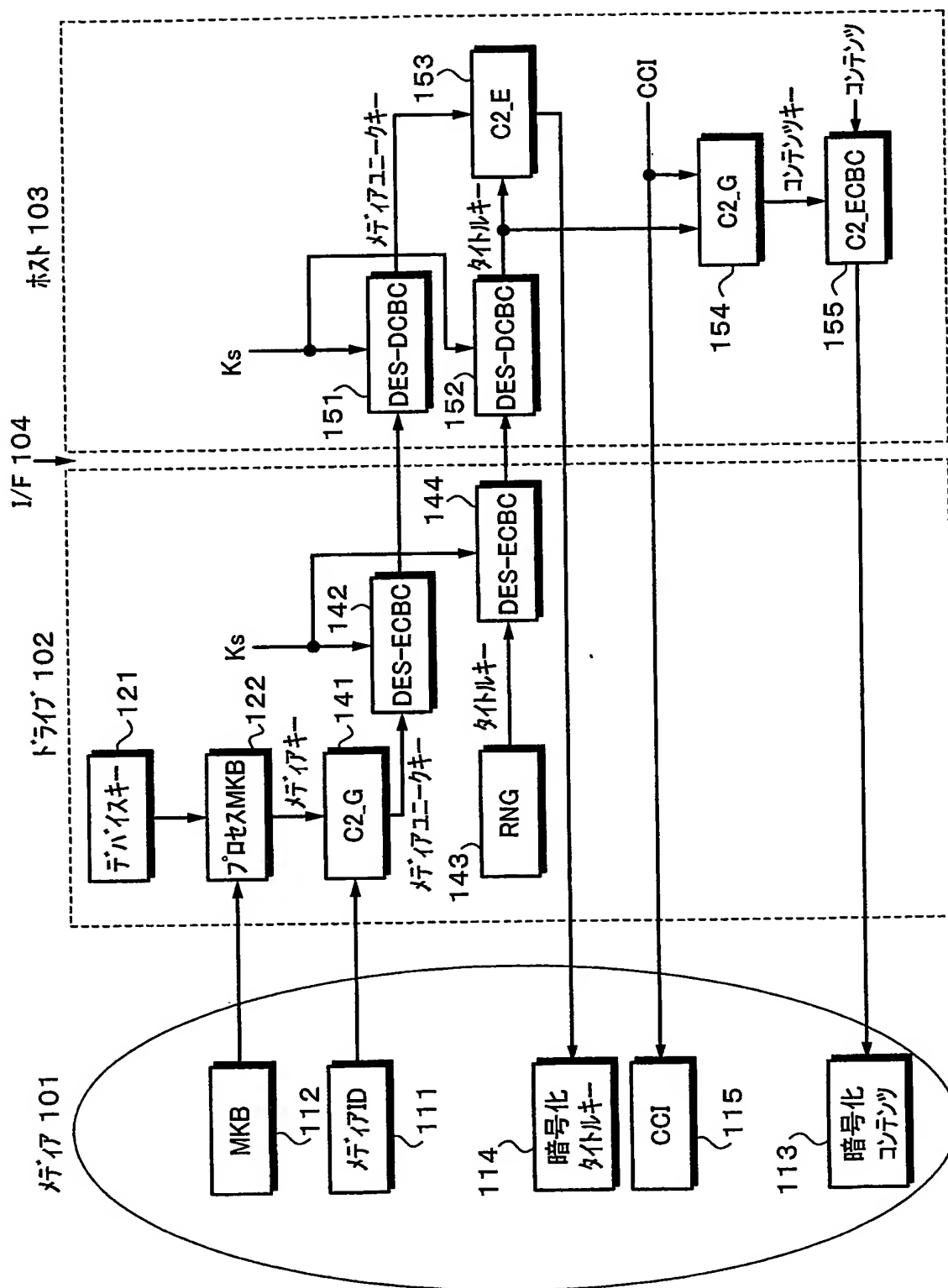
ドライブ102



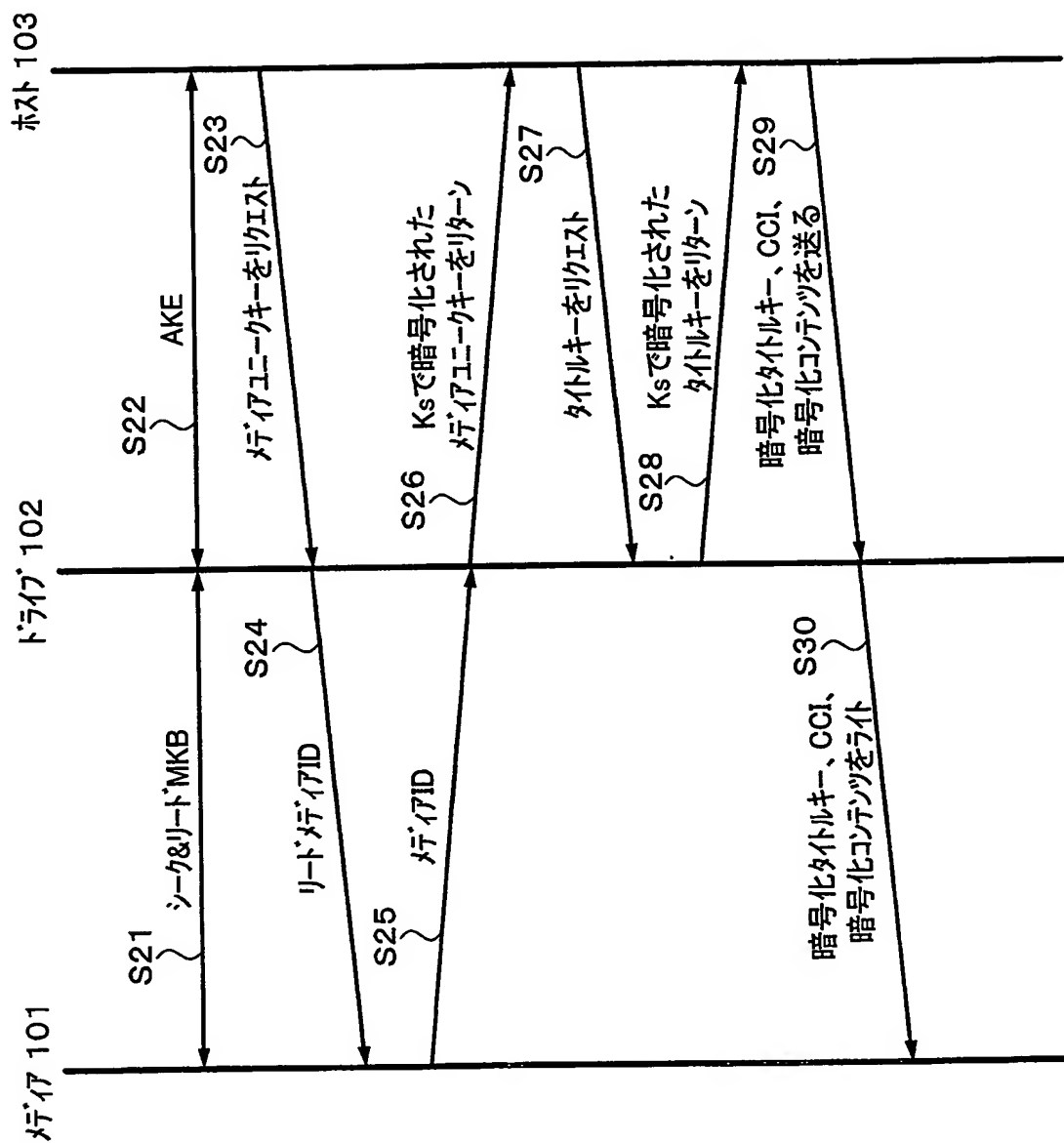
第7図



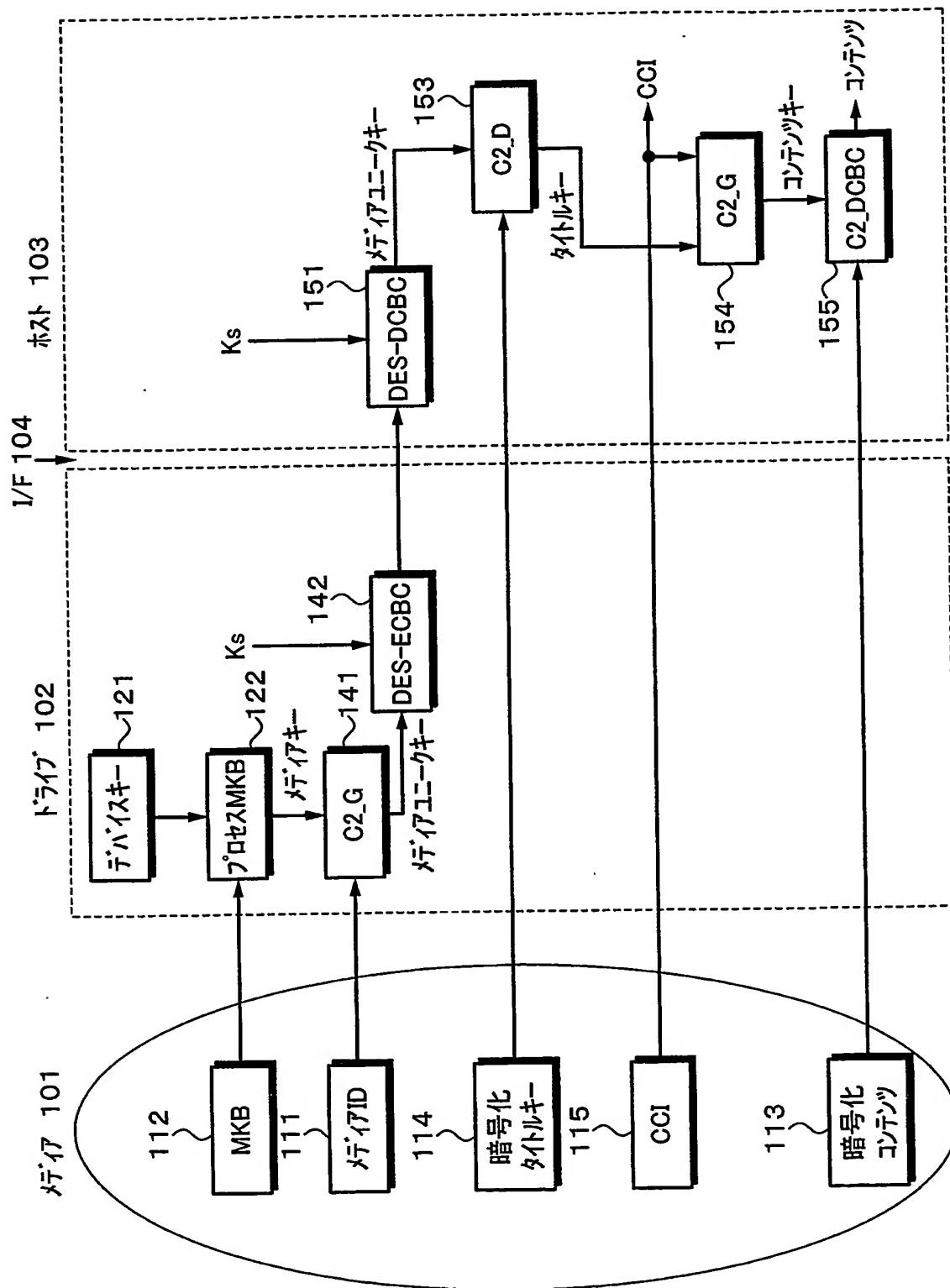
第8図



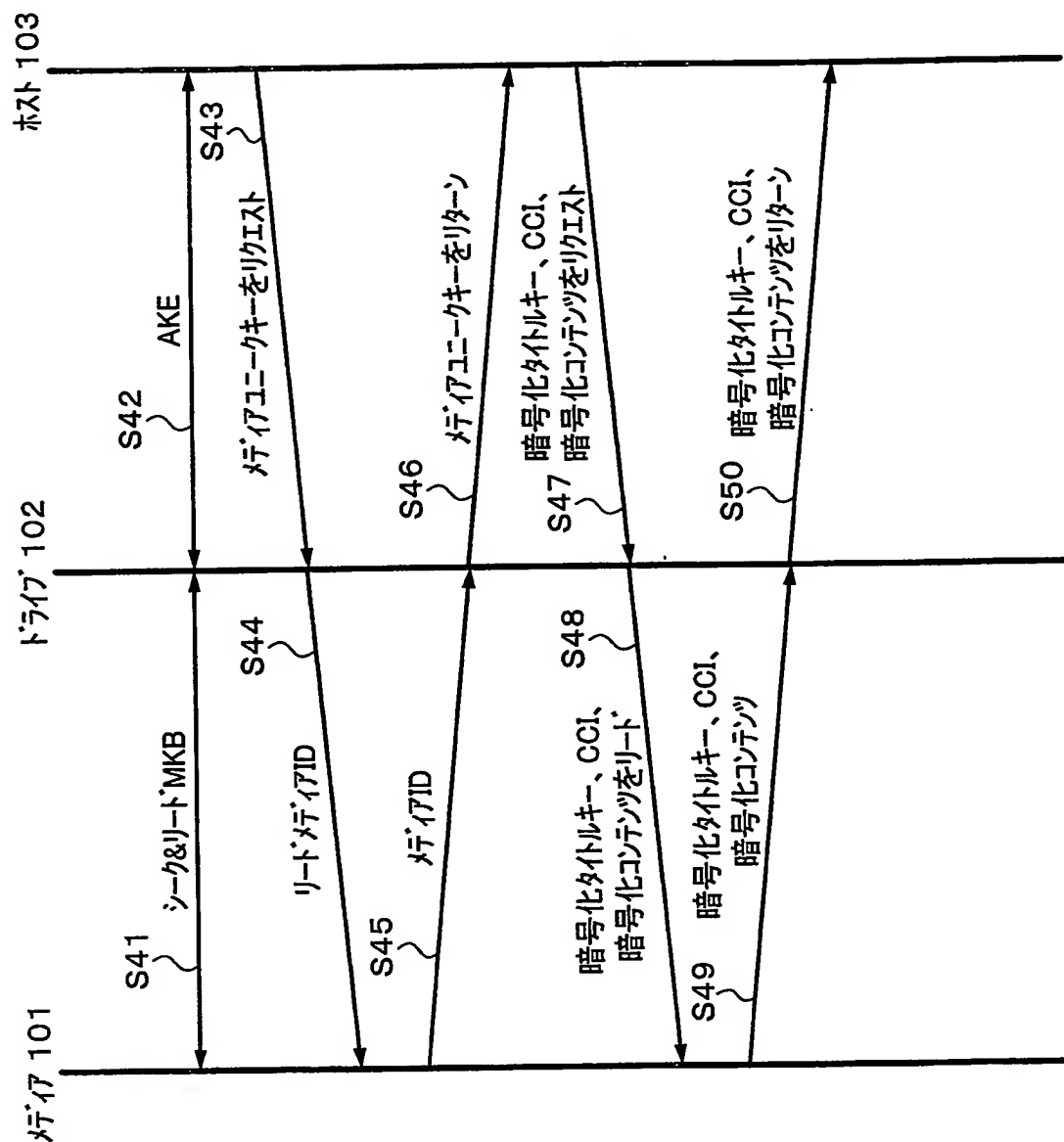
第9図



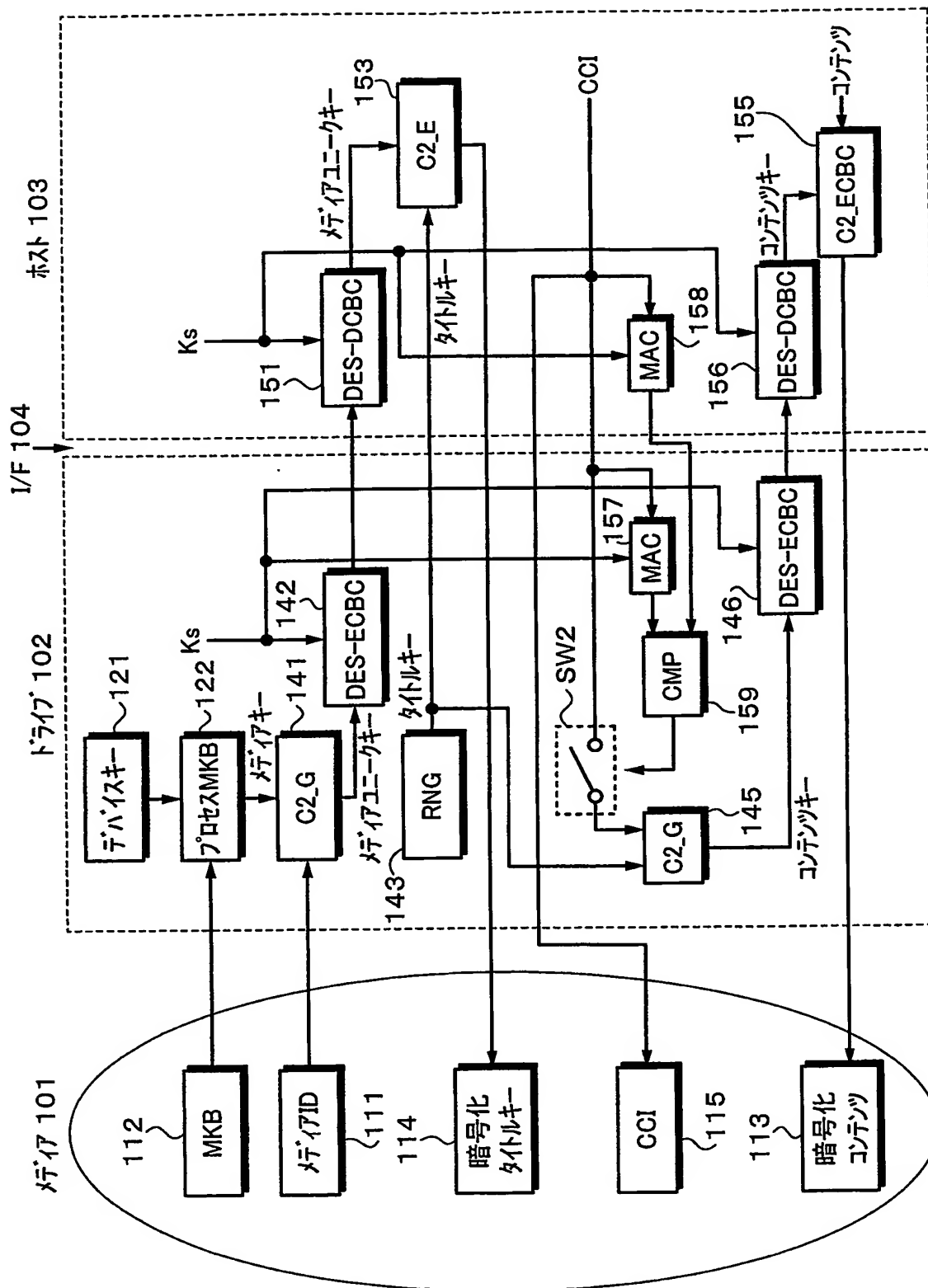
第10図



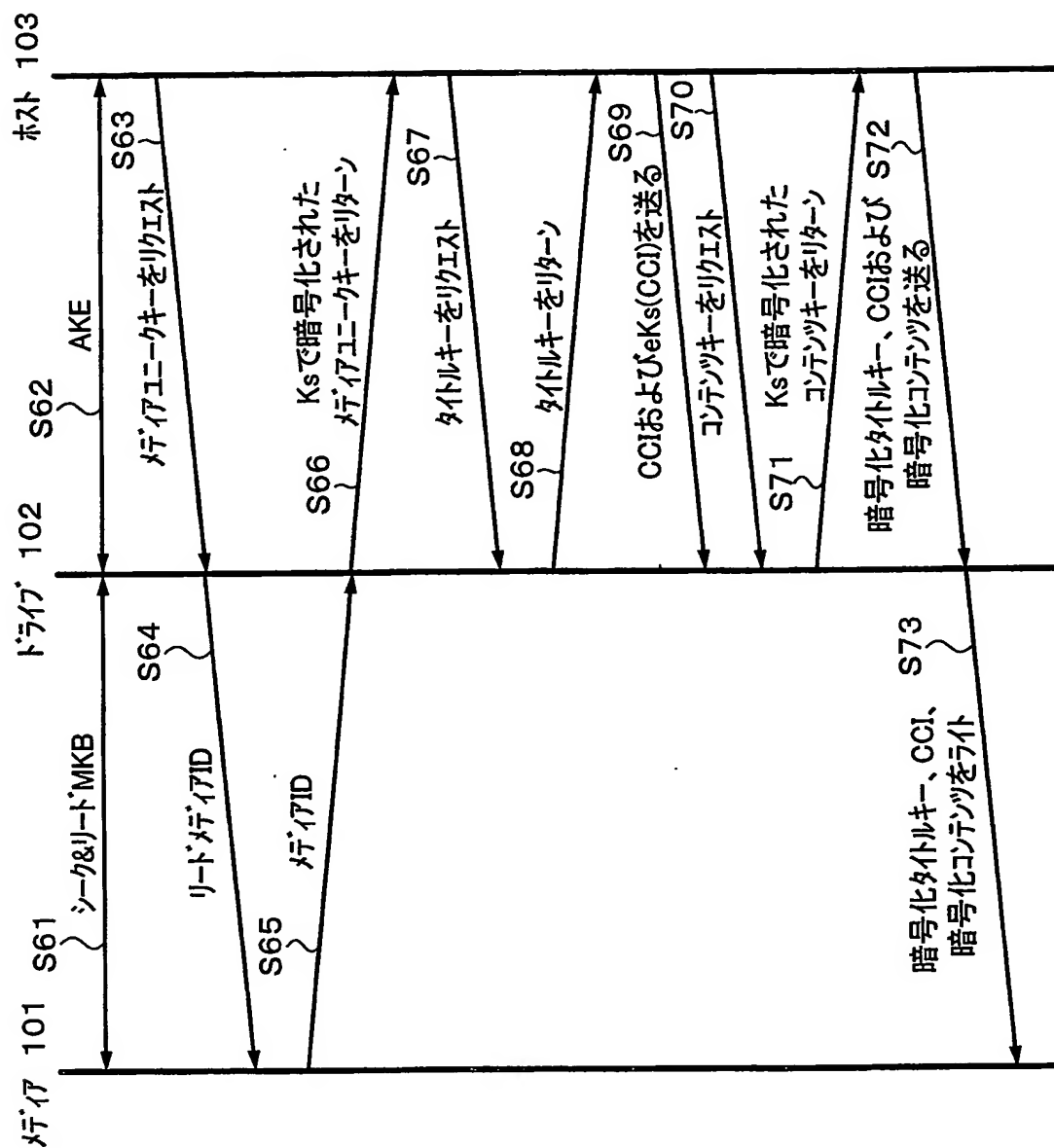
第11図



第12図



第13図



符号の説明

1	D V D メディア
2	レコーダ
3	プレーヤ
4	D V D ドライブ
4 a	インターフェース
5	ホスト
1 1	メディア I D
1 2	メディアキーブロック (M K B)
1 3	暗号化コンテンツ
4 2 , 5 2	M A C 演算ブロック
4 6	デバイスキー
4 6 a	デバイスキーの前半部.
4 7	D E S エンクリプタ
4 8	メディアユニークキー演算ブロック
4 9 , 4 9 a	D E S エンクリプタ
4 9 b	D E S デクリプタ
5 3	M A C を比較する比較
5 4	暗号化／複合モジュール
5 5	メディアユニークキー演算ブロック
1 0 1	メディア
1 0 2	ドライブ
1 0 3	ホスト
1 0 4	インターフェース
1 2 1	ドライブのデバイスキー

1 2 2 プロセス M K B

1 2 3、1 2 4、1 2 5 ドライブの M A C 演算ブロック

1 2 6、1 2 7、1 2 8 ドライブの乱数発生器

1 2 9 比較

1 3 1 ホストのデバイスキー

1 3 2 プロセス M K B

1 3 3、1 3 4、1 3 5 ホストの M A C 演算ブロック

1 3 6、1 3 7、1 3 8 ホストの乱数発生器

1 3 9 比較

1 4 1、1 5 4 C 2 __ G

1 4 2、1 4 4 D E S エンクリプタ

1 4 3 乱数発生器

1 5 1、1 5 2、1 5 6 D E S デクリプタ

1 5 3 C 2 __ E

1 5 5 C 2 __ E B C

1 5 7、1 5 8 M A C 演算ブロック

1 5 9 比較

S T 1 M A C 計算値が一致？

S T 2 スイッチを O N

S T 3 スイッチを O F F

S T 1 0 R E P O R T K E Y (M K B)

S T 1 1 メディアキー K m を計算

S T 1 2 リポーク？

S T 1 3 R E C E I V E (R b 1, R b 2)

S T 1 4 R E T U R N (e K m (R a 1 || R b 1), R a 1)

S T 1 5 R E T U R N (R a 2, R a 3)

ST 1 6 R E C E I V E
 $(eK_m(Rb\ 2 \parallel Ra\ 2), Rb\ 3)$

ST 1 7 同一のMAC?

ST 1 8 セッションキーの確定
 $(eK_m(Ra\ 3 \parallel Rb\ 3))$

ST 1 9 R E T U R N (エラー)

ST 2 0 R E P O R T K E Y (MKB)

ST 2 1 メディアキー K_m を計算

ST 2 2 リボーク?

ST 2 3 S E N D K E Y (Rb 1, Rb 2)

ST 2 4 R E P O R T K E Y
 $(eK_m(Ra\ 1 \parallel Rb\ 1), Ra\ 1)$

ST 2 5 同一のMAC?

ST 2 6 R E P O R T K E Y. (Ra 2, Ra 3)

ST 2 7 S E N D K E Y
 $(eK_m(Rb\ 2 \parallel Ra\ 2), Rb\ 3)$

ST 2 8 エラー?

ST 2 9 セッションキーの確定
 $(eK_m(Ra\ 3 \parallel Rb\ 3))$

INTERNATIONAL SEARCH REPORT

International application No.

/JP03/16226

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/32, G11B20/10, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/32, G11B20/10, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS), content, mutual, authentication, MKB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-331106 A (Matsushita Electric Industrial Co., Ltd.), 30 November, 2001 (30.11.01), Par. Nos. [0099] to [0115] & EP 1134964 A1 & CN 1313599 A & KR 2001092320 A & US 2002/0015494 A1 & TW 529020 A	1-9, 24, 25
Y	Makoto TATEBAYASHI et al., "Kiroku Media no Contents Hogo System", 2000 Nen The Institute of Electronics, Information and Communication Engineers Kiso Kyokai Society Taikai Koen Ronbunshu, 07 September, 2000 (07.09.00), pages 367 to 368, 2.2 MEB.o Mochiita Kagi Mukoka System, 4.2 Dosa Gaiyo	1-9, 24, 25

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
26 April, 2004 (26.04.04)

Date of mailing of the international search report
18 May, 2004 (18.05.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

T/JP03/16226

Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☒ Claims Nos.: 10-23
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/32, G11B20/10, G06F12/14

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/32, G11B20/10, G06F12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS)
content, mutual, authentication, MKB

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2001-331106 A (松下電器産業株式会社) 2001.11.30, 第99-115段落 & EP 1134964 A1 & CN 1313599 A & KR 2001092320 A & US 2002/0015494 A1 & TW 529020 A	1-9, 24, 25
Y	館林誠 他, 記録メディアのコンテンツ保護システム, 2000年電子情報通信学会基礎・境界ソサイエティ大会講演論文集, 2000.09.07, p.367-368, 2.2 MKBを用いた鍵無効化システム, 4.2動作概要	1-9, 24, 25

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

26.04.2004

国際調査報告の発送日

18.5.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正

5M 9364

電話番号 03-3581-1101 内線 3597

第 I 欄 請求の範囲の一部の調査ができないときの意見 (第 1 ページの 2 の続き)

法第 8 条第 3 項 (PCT 17 条 (2) (a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☒ 請求の範囲 10-23 は、従属請求の範囲であって PCT 規則 6.4(a) の第 2 文及び第 3 文の規定に従って記載されていない。

第 II 欄 発明の単一性が欠如しているときの意見 (第 1 ページの 3 の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。